



Sygate Enterprise Protection 5.0 Protection Agent User Guide

Documentation Build 2004

Published May 18, 2005

Copyright Information

Copyright© 2005 Sygate Technologies, Inc. and its licensors. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission of Sygate Technologies, Inc. Information in this document is subject to change without notice and does not constitute any commitment on the part of Sygate Technologies, Inc. Sygate Technologies, Inc. may have patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter of this document.

Furnishing of this documentation does not in any way grant you license to these patents, trademarks, copyrights, or any other intellectual property of Sygate Technologies, Inc.

Sygate, the Sygate 'S' Logo, Sygate Network Access Control, Sygate Enterprise Protection, Host Integrity, and AutoLocation Switching are registered trademarks or trademarks of Sygate Technologies, Inc.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Portions copyright © 1995-2005 Macromedia, Inc.

Portions derived from *Win32 Multithreaded Programming* by Aaron Cohen and Mike Woodring. Copyright © 1997 O'Reilly & Associates.

Portions copyright (c) 1997-1999 Ian Jackson. For a period of three years from receipt of this notice, Sygate shall, at your request, provide a copy of the **adns** source code at a fee equaling Sygate's reproduction cost.

Table of Contents

Preface	xi
Getting Help	xi
Sygate Enterprise Protection Documentation	xii
Intended Audience for the Sygate Protection Agent	xii
Getting Technical Support.....	xii
Third-Party Product Support	xiii
Chapter 1. Receiving and Installing the Protection Agent Software	1
Installing the Protection Agent Software	2
Uninstalling the Protection Agent Software	3
Chapter 2. Overview of the Protection Agent	5
The Sygate Policy Manager and the Agent.....	5
The Sygate Policy Manager and the Agent.....	6
What Does the Protection Agent Software Do?	6
Key Features	7
Some Options May Not Be Available.....	8
Determining Your Control Mode.....	8
Client Control.....	8
Server Control.....	9
Power User Mode.....	9
What is Your Control Mode?.....	9
Your Control Mode Can Change at Any Time	9
Chapter 3. Getting Around on the Protection Agent	11
Navigating the Main Console.....	11
Menus and Toolbar Buttons	14
Traffic History Graphs	15
Broadcast Traffic.....	15
Running Applications Field.....	15
Message Console.....	17
Status Bar	17
Status Light.....	17
Using the Menus and the Toolbar	17
Menus and Toolbars (Client Control)	18
Menus and Toolbars (Server Control).....	20
Menus and the Toolbar (Power User Mode).....	22
Using the System Tray Icon.....	24
What the System Tray Icon Tells You.....	25
What Does the Flashing System Tray Icon Mean?.....	26
The System Tray Icon Menu.....	27
Hiding and Displaying the System Tray Icon.....	29
Changing Locations	29
Importing and Exporting Profiles	30
Using the Security Rule Viewer.....	30
Server Rules	31

Agent Rules and Settings	31
Order of Priority of Agent versus Policy Manager Rules	32
How the Security Rule Viewer Works	32
Chapter 4. Protecting Your System.....	33
Scanning Your System.....	34
Types of Scans	35
Quick Scans	35
Stealth Scans	35
Trojan Scans	35
TCP Scans.....	35
UDP Scans.....	36
ICMP Scans	36
Setting the Access for Applications.....	36
Setting Advanced Options for Applications	37
Advanced Application Configuration (Client Control, Power User Mode)	38
To Set Up Advanced Configuration:.....	38
Configuring the Agent's Settings	40
General Tab.....	41
Hide Sygate Protection Agent System Tray Icon	41
Automatically load Sygate Security Agent at startup.....	42
Block Network Neighborhood traffic while in screensaver mode	42
Hide notification messages	42
Beep before notify.....	42
Display messages for __ seconds.....	42
Set Password	42
Ask password while exiting.....	43
Network Neighborhood Tab.....	43
Network Interface	44
Allow others to share my files and printer(s)	44
Security Tab.....	44
Enable Intrusion Prevention System.....	45
Enable port scan detection	45
Enable driver level protection	46
Enable stealth mode browsing.....	46
Enable DoS detection.....	46
Block Universal Plug and Play Traffic	46
Automatically block attacker's IP address for... second(s).....	46
Block all incoming traffic while the service is not loaded	46
Allow initial traffic.....	47
Enable anti-MAC spoofing.....	47
Enable anti-IP spoofing	47
Enable OS fingerprint masquerading.....	47
NetBIOS protection	47
Allow Token Ring Traffic.....	48
Enable smart DNS.....	48
Enable smart DHCP.....	48
Enable smart WINS.....	48

E-Mail Notification Tab	48
Do Not Notify.....	49
Notify Immediately	49
After Every __ Minutes.....	49
My E-Mail Server Requires Authentication.....	50
Test E-Mail Notification	50
Log Tab	50
Enable Log.....	51
Maximum log file size.....	51
Save log file for the past xx days.....	51
Clear Logs.....	51
IEEE 802.1x Authentication Tab	52
Enable IEEE 802.1x Authentication	52
Enable Transparent Mode	53
Setting Up Advanced Rules	53
General Tab.....	53
Rule Description.....	54
Block this traffic	54
Allow this traffic.....	54
Apply Rule to Network Interface	54
Apply this rule during Screensaver Mode.....	55
Record this traffic in “Packet Log”	55
Rule Summary field.....	55
Hosts Tab.....	55
All addresses.....	56
MAC addresses	56
IP Address(es).....	56
Subnet	56
Rule Summary field.....	56
Ports and Protocols Tab.....	56
Protocol	57
Traffic Direction.....	58
Rule Summary field.....	58
Scheduling Tab.....	58
Enable Scheduling.....	59
Beginning At	59
Duration.....	59
Rule Summary field.....	60
Applications Tab.....	60
Display selected applications only	60
Applications	60
Select All.....	61
Clear All.....	61
Browse	61
Rule Summary field.....	61
Viewing Server and Agent Rules	61
The Security Rule Viewer.....	61
Order of Priority for Agent Rules versus Server Rules	62

Chapter 5. Monitoring and Logging.....	63
Viewing Logs	64
Traffic Log	65
Icons for the Traffic Log	65
Traffic Log Parameters and Description	65
Description and Data Fields for the Traffic Log.....	66
Packet Log.....	67
Icons for the Packet Log.....	67
Packet Log Parameters and Description.....	67
Packet Decode and Packet Dump for the Packet Log.....	68
System Log.....	68
Icons for the System Log.....	68
System Log Parameters and Description.....	69
Description and Data Fields for the System Log.....	69
Security Log	69
Icons for the Security Log	69
Security Log Parameters and Description	70
Description and Data Fields for the Security Log.....	71
Behavior Log.....	72
Enabling and Clearing Logs.....	73
Back Tracing Logged Events.....	74
Filtering Logged Events	75
Saving Logs	76
Stopping an Active Response.....	76
Responding to Access Status Pop-up Messages	77
Chapter 6. Messages and Warnings.....	79
Why Did I Get a Pop-up Message?	80
New Application Pop-up.....	80
What Does This Mean?	80
Detail.....	81
What Should I Do?	81
Changing the Status of an Application.....	82
Changed Application Pop-up Messages.....	82
What Does This Mean?	83
Detail.....	83
What Should I Do?	83
Changing the Status of an Application.....	83
Fast User Switch Pop-up Message	83
What Does This Mean?	84
What Should I Do?	84
Automatic Update Notification.....	84
Trojan Horse Warning.....	85
What Does This Mean?	85
What Should I Do?	85
Why Did I get a Security Notification?.....	85
Blocked Application Notification.....	86
Security Alert Notification.....	86

Why Did I Get a Warning Message?	86
Your Agent Does An Automatic Download.....	87
You May Be Blocked From the Network	87
Glossary	89
Index	111

List of Tables

Table 1.	Running Applications Field	16
Table 2.	Agent Menus (Client Control)	18
Table 3.	Agent Menus (Server Control)	20
Table 4.	Agent Menus (Power User)	22
Table 5.	System Tray Icon Colors	25
Table 6.	System Tray Icon Appearance	25
Table 7.	System Tray Icon Menu	27
Table 8.	Traffic Log Icons	65
Table 9.	Traffic Log Parameters and Description	65
Table 10.	Packet Log Icons	67
Table 11.	Packet Log Parameters and Description	67
Table 12.	System Log Icons	68
Table 13.	System Log Parameters and Description	69
Table 14.	Security Log Icons	69
Table 15.	Security Log Parameters and Description	70
Table 16.	Agent Behavior Log Parameters and Description	72
Table 17.	Agent Application Access Status	77
Table 18.	Pop-up: Remember My Answer?	82

List of Figures

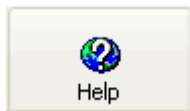
Figure 1.	Main Console in Client Control	12
Figure 2.	Main Console in Server Control	13
Figure 3.	Main Console in Power User Mode	14
Figure 4.	Traffic History Graph.....	15
Figure 5.	Security Rule Viewer	31
Figure 6.	Applications List.....	38
Figure 7.	Advanced Application Configuration	39
Figure 8.	Options: General Tab.....	41
Figure 9.	Options: Network Neighborhood Tab.....	44
Figure 10.	Options: Security Tab.....	45
Figure 11.	Options: E-Mail Notification Tab.....	49
Figure 12.	Options: Log Tab.....	51
Figure 13.	Options: IEEE 802.1x Authentication Tab	52
Figure 14.	Advanced Rules: General Tab.....	54
Figure 15.	Advanced Rules: Hosts Tab	55
Figure 16.	Advanced Rules: Ports and Protocols Tab.....	57
Figure 17.	Advanced Rules: Scheduling Tab.....	59
Figure 18.	Advanced Rules: Applications Tab.....	60
Figure 19.	Security Rule Viewer	62
Figure 20.	Log viewer	71

Preface

This guide describes how to install and use the Sygate Protection Agent, one of the components of the Sygate Enterprise Protection software. It also describes the relationship of the Protection Agent to other components of the Sygate Enterprise Protection suite of products.

Getting Help

From the Agent console, you can choose **Help | Help topics** from the menu bar, click the **Help** button, or press **F1**.



The information in this help system is also available in the *Sygate Protection Agent User Guide* in Adobe's PDF format for easy printing. You can download the *Sygate Protection Agent User Guide* from the Sygate Technologies web site at <http://www.sygate.com>.

For late-breaking news about known problems with this release, refer to the `Readme.txt` file that is included with this software.

This document, the *Protection Agent User Guide*, describes how to install and use the Agent software. It also describes the relationship of the Agent to other components of the Sygate Enterprise Protection suite of products, including the Sygate Policy Manager. The Policy Manager is defined as "A centralized point of control over all Sygate Protection and Enforcement Agents that enables network administrators to define and distribute security policies, collect logs, and maintain the integrity of the corporate network."

In this guide you will find information about:

- Receiving the Agent software
- Installing the Agent software
- Understanding the Agent software

- Getting around the Agent interface
- Testing your system's vulnerability
- Protecting your system
- Monitoring your system through logs
- Working with messages and warnings

Sygate Enterprise Protection Documentation

The Sygate Enterprise Protection suite includes the following documentation:

- *Online Help*—All components of Sygate Enterprise Protection have help files. These help files provide the same information as the printed documentation, which is available in PDF format from the Sygate web site at <http://www.sygate.com/support/index.htm>.
- *Sygate Enterprise Protection Policy Manager Installation Guide*—Describes how to install and configure the Policy Manager, Sygate Protection Agent, and Sygate Enforcement Agent (PDF format).
- *Sygate Enterprise Protection Policy Manager Administration Guide*—Describes how to administer the Policy Manager, Sygate Protection Agent, and Sygate Enforcement Agent (PDF format).
- *Sygate Enforcer Installation and Administration Guide*—Describes how to install, configure, and administer the Sygate Gateway Enforcer, Sygate LAN Enforcer, and the Sygate DHCP Enforcer.
- *Sygate Protection Agent User Guide*—Describes how to install and use the Sygate Protection Agent (PDF format)
- *Sygate Enforcement Agent User Guide*—Describes how to use the Sygate Enforcement Agent (PDF format).

Intended Audience for the Sygate Protection Agent

This documentation is written for end users of the Agent software.

This documentation assumes that the user is familiar with the basic functioning of Windows operating systems and standard Windows items, such as buttons, menus, toolbars, windows, etc. Further, this documentation assumes that the user has a network or an Internet connection, whether through a local area network, DSL connection, dial-up modem, wireless access point, or other connection method.

Getting Technical Support

Sygate Technologies provides a variety of service and support programs. Contact Enterprise Support through its web site, by email, or by telephone.

Sygate web site: www.sygate.com/support
Email address: EnterpriseSupport@sygate.com
Telephone number: (510) 742-2622
Toll free number: (877) TECH-800 (832-4800)

Third-Party Product Support

If you obtained this product from a hardware or software company other than Sygate Technologies directly, your software license as well as all service and support should be obtained through the vendor. Check the addendum provided with the package for service and support information.

Chapter 1. Receiving and Installing the Protection Agent Software

The Agent software can be distributed to you in a number of ways. You may need to take some action to go and get the software, or the software may already be installed.

- **Web download**—The installation file is placed by your administrator in a location on the Web or a server on your Extranet. You navigate to that location to unzip and run the `Setup.exe` program to install the Agent. With this type of installation, you may be prompted for your license information, location of the software on your hard drive, and so on, as described in “Installing the Protection Agent Software,” although your system administrator may have already made some of those choices for you.
- **Server distribution**—You receive an email message, or, other pointer to the `Setup.exe` program that is in a folder that you can reach on your Intranet or Extranet. Run that program and it installs the Agent. With this type of installation, you may be prompted for your license information, location of the software on your hard drive, and so on, as described in “Installing the Protection Agent Software,” although your system administrator may have already made some of those choices for you.
- **Server login script**—Your security administrator sets up a login script that automatically installs the Agent software. With this type of installation, you are not prompted usually for anything; the system administrator probably makes all choices for you. You may be aware the Agent is installing, or, your administrator may do the installation in “silent” mode hidden from view.
- **CD distribution**—Your security administrator puts the Agent software onto a CD-ROM. You then run the `Setup.exe` program to install the software, as described in “Installing the Protection Agent Software.”
- **Image file**—The Agent package is included in an image file that contains a complete system setup, including operating system and applications. In this case, you probably do not do any installation yourself, but simply use the Agent.
- **Software management tools**—Your system administrator uses a tool such as Microsoft System Management Software, IBM Tivoli, or HP OpenView to package

the Agent into an automatic installation. In this case, you probably do not do any installation yourself, but simply use the Agent.

The Agent software can be distributed to you in a number of ways. You may need to take some action to go and get the software, or the software may already be installed.

- **Web download**—The installation file is placed by your administrator in a location on the Web or a server on your Extranet. You navigate to that location to unzip and run the `Setup.exe` program to install the Agent. With this type of installation, you may be prompted for your license information, location of the software on your hard drive, and so on, as described in “Installing the Protection Agent Software,” although your system administrator may have already made some of those choices for you.
- **Server distribution**—You receive an email message, or, other pointer to the `Setup.exe` program that is in a folder that you can reach on your Intranet or Extranet. Run that program and it installs the Agent. With this type of installation, you may be prompted for your license information, location of the software on your hard drive, and so on, as described in “Installing the Protection Agent Software,” although your system administrator may have already made some of those choices for you.
- **Server login script**—Your security administrator sets up a login script that automatically installs the Agent software. With this type of installation, you are not prompted usually for anything; the system administrator probably makes all choices for you. You may be aware the Agent is installing, or, your administrator may do the installation in “silent” mode hidden from view.
- **CD distribution**—Your security administrator puts the Agent software onto a CD-ROM. You then run the `Setup.exe` program to install the software, as described in “Installing the Protection Agent Software.”
- **Image file**—The Agent package is included in an image file that contains a complete system setup, including operating system and applications. In this case, you probably do not do any installation yourself, but simply use the Agent.
- **Software management tools**—Your system administrator uses a tool such as Microsoft System Management Software, IBM Tivoli, or HP OpenView to package the Agent into an automatic installation. In this case, you probably do not do any installation yourself, but simply use the Agent.

Installing the Protection Agent Software

If your system administrator has not already installed the software on your computer, you have probably been given instructions on where to find the Agent software and how to install it yourself.

To install the software:

1. Run **Setup.exe**.
The Agent Setup window appears.
2. Click **Next**.
The License Agreement dialog box appears. Scroll through the agreement to make sure that you agree with its terms.
3. Click **I accept the license agreement** if you agree, then click **Next**.
The Destination Folder dialog box appears.
4. Click **Next** to accept the default location for the Agent files or click **Browse** to select a different location.
The Ready to Install the Application dialog box appears.
5. Click **Next**.
If you are updating a previous installation, the Upgrade Installation dialog box appears. If you want to keep the previous configuration, click **Yes**. Otherwise, click **No**.
The Updating System window appears while the files are copied to your system, followed by the Finish window.
6. Click **Finish**.
The Installer Information dialog box appears, telling you that you must restart your computer to begin using the Agent.
7. Click **Yes** to reboot your system and begin using the Agent, or click **No** if you plan to restart manually later.

Uninstalling the Protection Agent Software

If you need to uninstall the Protection Agent software:

1. Click the **Start Menu** on your task bar.
2. Click **Settings | Control Panel | Add/Remove Programs**.
3. Click **Sygate Protection Agent 5.0**.
4. Click **Remove**. The Windows uninstaller guides you through the process.

Note: Your administrator may have set a password that you must enter to uninstall the software. If so, enter it in the Uninstall Password dialog box. If you do not enter the correct password, you cannot uninstall the Agent software.

Chapter 2. Overview of the Protection Agent

The Sygate Protection Agent (the Agent) is security software and one of the components in the Sygate Enterprise Protection software suite. Once installed, the Agent provides a customizable firewall that protects the computer from intrusion and misuse, whether malicious or unintentional. It detects and identifies known Trojans, port scans, and other common attacks. In response, it selectively allows or blocks *traffic*, various networking services, applications, ports, and components.

The Agent uses *security policies*, which include security rules and *security settings*, to protect an individual computer from network traffic that can cause harm. Because the Agent is deployed as part of the Sygate Enterprise Protection security suite, it works with other security components to protect the corporate network. For each application or service that tries to gain access through your network connection, the Agent uses security rules to determine whether that application is allowed access.

The Sygate Policy Manager and the Agent

The Agent communicates with and receives security instructions from the Sygate Policy Manager, another software component of the Sygate Enterprise Protection software. Your system administrator has defined the security policies that the Policy Manager distributes to the Agents.

The Policy Manager serves as a centralized point of control over all Agents. It enables system administrators to define and distribute security policies, collect logs, and maintain the integrity of the corporate network. It deploys security policies to the Agents, sends out updated intrusion detection signatures, and handles security issues for the enterprise. Your Agent's policies are automatically updated when it first connects with the Policy Manager, and periodically while connected. As an integral part of enterprise security, the Agent also keeps track of attempted violations of security policies, and transfers this information in logs to the Policy Manager.

Your system administrator makes decisions that directly affect your use of the Agent. They may have given you more or less control over your own security policies depending upon the control mode and location of your Agent.

The Sygate Protection Agent (the Agent) is security software and one of the components in the Sygate Enterprise Protection software suite. Once installed, the Agent provides a customizable firewall that protects the computer from intrusion and misuse, whether malicious or unintentional. It detects and identifies known Trojans, port scans, and other common attacks. In response, it selectively allows or blocks *traffic*, various networking services, applications, ports, and components.

The Agent uses *security policies*, which include security rules and *security settings*, to protect an individual computer from network traffic that can cause harm. Because the Agent is deployed as part of the Sygate Enterprise Protection security suite, it works with other security components to protect the corporate network. For each application or service that tries to gain access through your network connection, the Agent uses security rules to determine whether that application is allowed access.

The Sygate Policy Manager and the Agent

The Agent communicates with and receives security instructions from the Sygate Policy Manager, another software component of the Sygate Enterprise Protection software. Your system administrator has defined the security policies that the Policy Manager distributes to the Agents.

The Policy Manager serves as a centralized point of control over all Agents. It enables system administrators to define and distribute security policies, collect logs, and maintain the integrity of the corporate network. It deploys security policies to the Agents, sends out updated intrusion detection signatures, and handles security issues for the enterprise. Your Agent's policies are automatically updated when it first connects with the Policy Manager, and periodically while connected. As an integral part of enterprise security, the Agent also keeps track of attempted violations of security policies, and transfers this information in logs to the Policy Manager.

Your system administrator makes decisions that directly affect your use of the Agent. They may have given you more or less control over your own security policies depending upon the control mode and location of your Agent.

What Does the Protection Agent Software Do?

Your Agent protects your individual computer from network traffic that can cause it harm. It does this by applying one of three *firewall rules*:

- **Allow:** The Agent ***Allows*** some traffic to flow. This is usually traffic that is known to be “safe”, either because you are in Server Control and your system administrator has defined it to be safe, or because you are in Client Control and you have made that determination yourself. Examples of traffic normally classified as safe include Outlook, Internet Explorer, Netscape Navigator, Outlook Express, and other common networking and communications software.

- **Block:** The Agent **Blocks** some traffic. This is usually traffic that is known to be problematic or dangerous to your computer. If you are in Server Control, your system administrator has already made some decisions in this area that will protect your computer and that will block traffic that is known or thought to be dangerous.
- **Ask:** The Agent **Asks** whether incoming and outgoing traffic is allowed to access your computer or an organization's network resources. When the Agent is in Client Control, it initially asks you whether to permit your applications to access network resources. Optionally, it remembers your responses, so that you do not have to tell it again.

Firewall rules allow the Agent to systematically **Allow**, **Block**, or **Ask** about what action to take on incoming traffic from specific IP addresses and ports. The configuration of those rules with other security settings results in a security agent that protects your computer.

Key Features

The Agent can be used in a variety of networking environments. Some of these environments include direct connection to the local LAN or wireless network, remote connection using Virtual Private Network (VPN) or dial-up, or completely disconnected from any network. Its features, particularly in combination with the Management Server, are powerful and flexible.

- **Heartbeat synchronization**—The Agent is an integral part of enterprise security. It sends status logs and receives security policies from the Management Server on an ongoing basis. This constant checking between the Agent and Management Server is called the heartbeat. The default heartbeat is every five minutes, but can be changed from the Policy Manager. If a new policy is defined for the group to which an Agent belongs, it receives that new policy at the next heartbeat.
- **Customized security policy**—Each Agent is a member of a working group (For example, Marketing, Sales, VPN Users). The system administrator defines security policies for each group, and they are automatically updated to the Agents who are members of that group. If an end user moves from one group to another, the security policies for the new group automatically apply to that user's Agent upon the next heartbeat.
- **AutoLocation switching**—The Agent can be customized by the Policy Manager to automatically recognize the environment or location in which it is working, and immediately switch to the security policy that has been created for that location. For example, you might connect from home or the office. The Agent will detect the location and automatically switch locations. Each Agent can be configured to have a variety of locations predefined, with each location providing an appropriate security policy.
- **Host integrity**—Each Agent can be required to have certain applications running (virus protection, for example) and to be blocked from network access until that application is up to date and running on the Agent machine. If the Agent fails a Host Integrity check, it can then be automatically routed to the appropriate location for

downloading and installing the updates that are needed. Those updates can include operating system patches, security firewall software, and other programs your administrator determines are required for your computer.

- **Multiple types**—The Agent is designed to work on most Windows-based computers, including servers and workstations. The AutoLocation Switching feature is normally deployed on remote computers or laptops, but can be deployed on all installations.
- **Works with the Enforcer**—The Agent can also be deployed in conjunction with the Enforcer, which adds an additional protective layer of security. It ensures that all computers connecting to the network paths it protects are running the Agent and have the proper security policy implemented.

Some Options May Not Be Available

Depending on what your system administrator decides, the features on the Agent console may change at times. The Agent can be either completely invisible for some users, display a partial set of features, or display a full user interface for yet another set of users. These differences depend on the control mode under which your Agent is operating, or the location in which you are using the Agent.

This help describes all features and options that the Agent supports. You or your company may have purchased a limited license that provides fewer options, or your system administrator may have disabled certain options for security reasons.

➡ **Option Alert:** This icon appears for options that are disabled or only available for a particular control mode.

Determining Your Control Mode

To protect your computer from the latest attacks and vulnerabilities that exist, your system administrator may change the *control mode* of your system. Each mode provides different levels of control over the Agent's security policy.

The Agent operates in one of three control modes:

- Client Control
- Server Control
- Power User Mode

Client Control

Client Control mode gives you the most control over your security settings. Client control is usually given to engineers or installed on computers that are used to test software. If you connect to your corporate network from home, you may have a client-controlled Agent on

your laptop. If you use the same laptop to connect to the network at work, then the Agent may change to *Server Control* mode when you arrive at work. This is an example of the Agent option called AutoLocation Switching.

Server Control

Server Control mode gets its rules and security settings from the Management Server. Although you can't change these settings from the Agent, this server-controlled Agent is likely to be more secure than a client-controlled Agent.

Power User Mode

Power User mode is a hybrid control mode that it is a mixture of the security policy that you set yourself, with an overlay of the policy set for you by the system administrator. Your system administrator decides in advance which settings you can change. You can see the how rules and settings apply in the Security Rule Viewer.

What is Your Control Mode?

There is no obvious way to tell which mode your Agent is in. You can, however, tell which control mode your Agent is using by examining the menus and toolbars that appear on the main console. For example, if in *Server Control* mode, you will not see a Security Test button on the toolbar. If you click the Tools menu and see Security Rule Viewer, your Agent is in *Power User* mode. When in *Client Control* mode this menu option changes to Advanced Rules instead of Security Rule Viewer.

Your Control Mode Can Change at Any Time

Your Agent is a part of a larger environment. In that larger, enterprise environment, your security administrator is responsible for protecting against the latest attacks and vulnerabilities that exist. To protect your computer, your system administrator may change the control mode or control mode's default settings on your Agent at any time. Once the system administrator makes changes on the Policy Manager level, these protective strategies and settings are implemented automatically on your Agent at the next *heartbeat*, or regular connection your Agent has with the Policy Manager.


Your security policies and firewall rules may also change based on changes at the Policy Manager level. The advantage of this is that your system administrator keeps track of security threats and implements protective strategies and settings automatically.

These changes are transparent to you, in the sense that you need take no action to implement them. However, you may see a change in your user interface, or in the applications that you use to access the network.

Chapter 3. Getting Around on the Protection Agent

The Agent is designed to start automatically when you turn on your computer. To configure your Agent, or review logs of potential attacks on your Agent, you open the Agent Console.


You can open the Agent in two ways:

- **System tray icon**—Double-click the icon  on the right side of the taskbar, or right-click it and click **Sygate Protection Agent 5.0**.
- **Start menu**—Click **Start | All Programs | Sygate Protection Agent**.

Either method opens the *main console*, that is the control center for the Agent. You can navigate the main console using the menus and toolbars.

The Agent is designed to start automatically when you turn on your computer. To configure your Agent, or review logs of potential attacks on your Agent, you open the Agent Console.

You can open the Agent in two ways:

- **System tray icon**—Double-click the icon  on the right side of the taskbar, or right-click it and click **Sygate Protection Agent 5.0**.
- **Start menu**—Click **Start | All Programs | Sygate Protection Agent**.

Either method opens the *main console*, that is the control center for the Agent. You can navigate the main console using the menus and toolbars.

Navigating the Main Console

Once you open the Agent, you see the main console. The main console provides real-time network traffic updates, online status, and Policy Manager updates. You can also view logs, help files, a list of applications, and access various rules and options.

The main console changes depending on the different control modes of the Agent. You can be in one of the following control modes:

- Client Control
- Server Control
- Power User

The Agent interface is resizable, so you can view it as a full-screen or part-screen image.

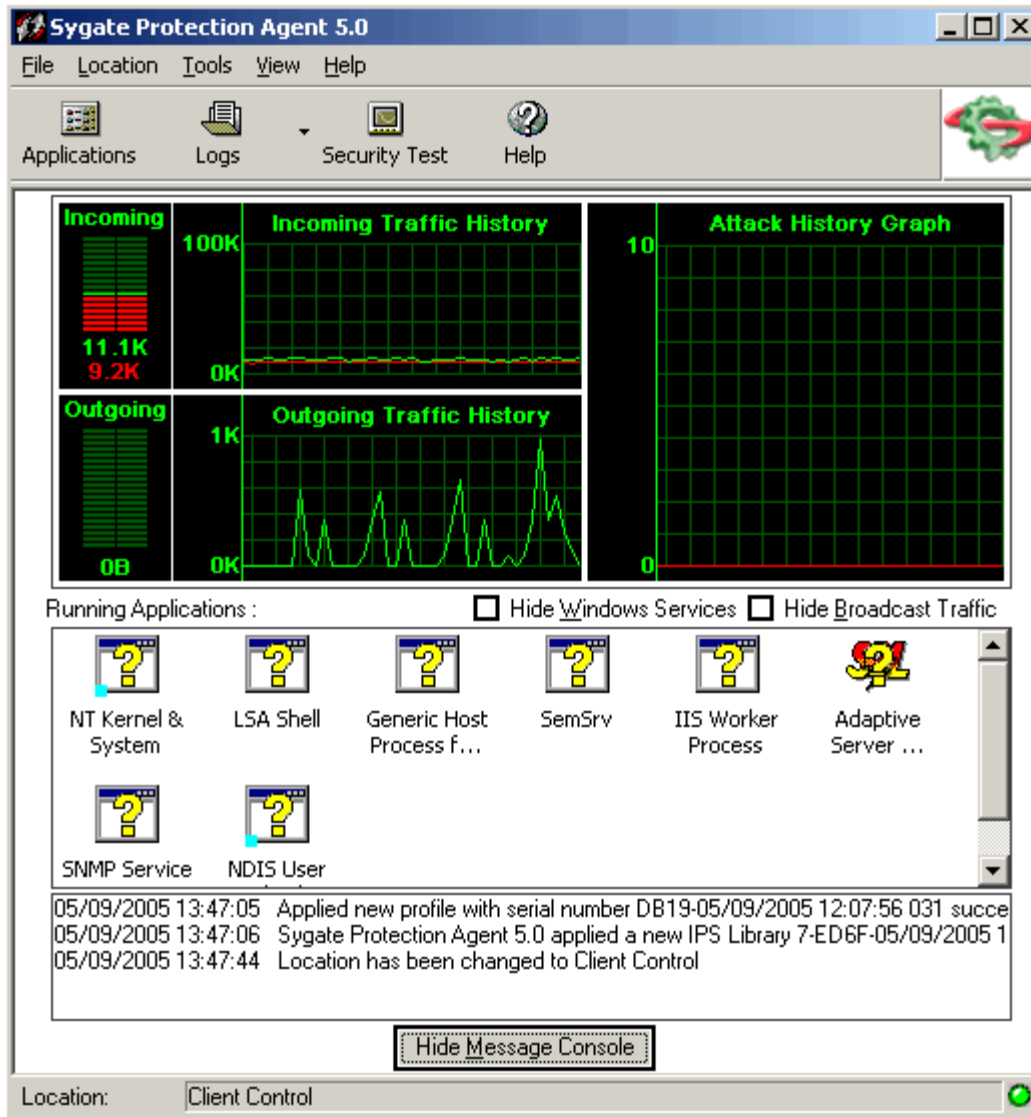


Figure 1. Main Console in Client Control

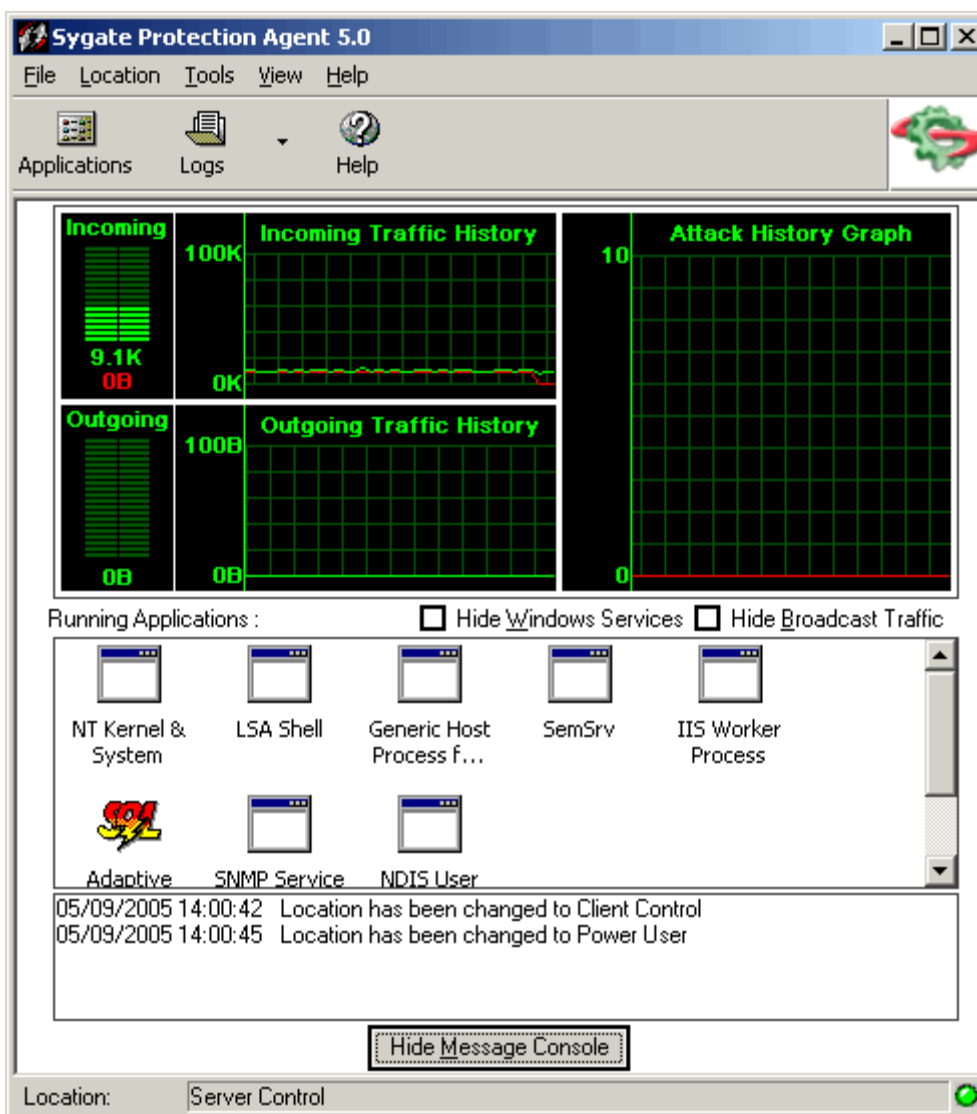


Figure 2. Main Console in Server Control

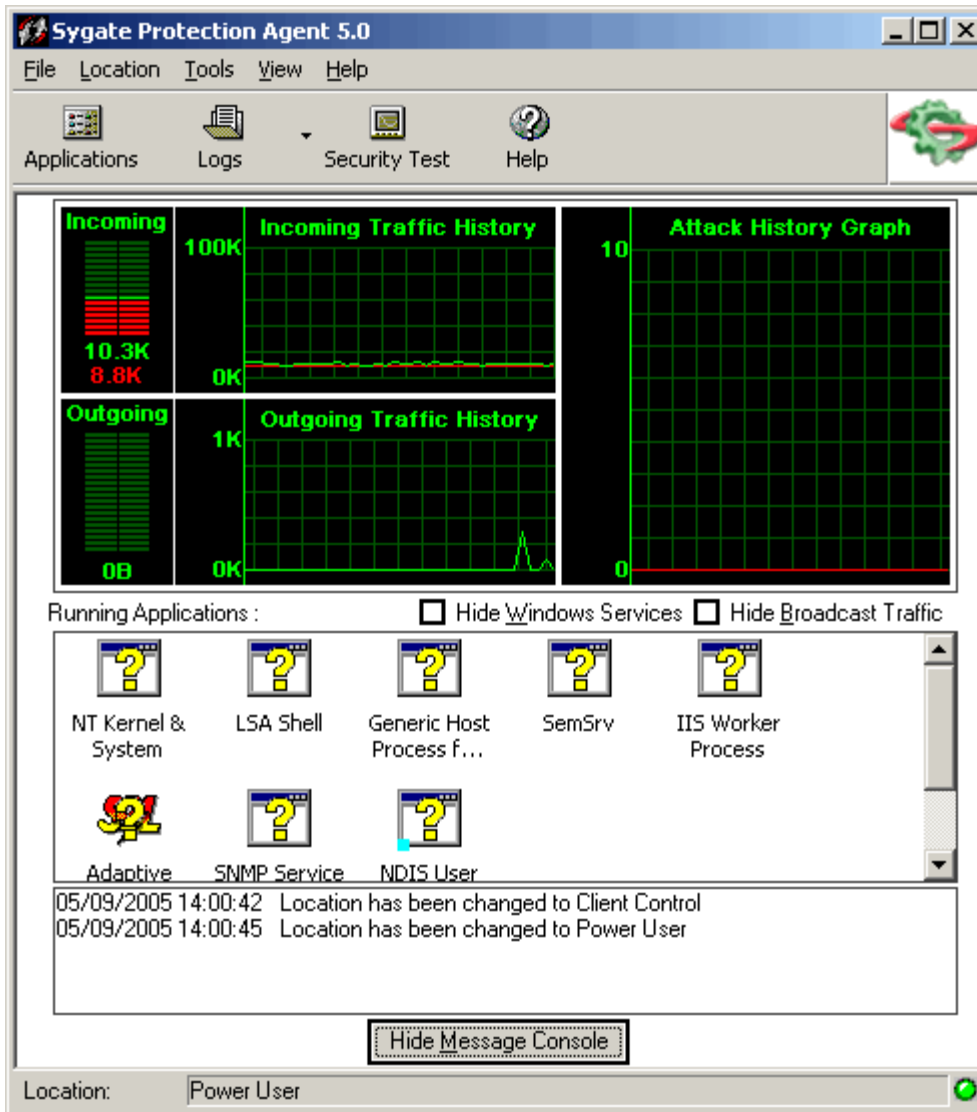


Figure 3. Main Console in Power User Mode

Menus and Toolbar Buttons

The top of the screen displays a standard menu and toolbar with options that vary depending upon the control mode—Client Control, Server Control, or Power User mode—of your Agent. The toolbar buttons can be used to quickly access logs, view the Help file, or test your system.

Traffic History Graphs

Below the toolbar are the Traffic History graphs.

The Traffic History graphs produce a real-time picture of the last two minutes of your traffic history. The graphs reload new information every second, providing instant data, as measured in bytes, about your incoming and outgoing network traffic.

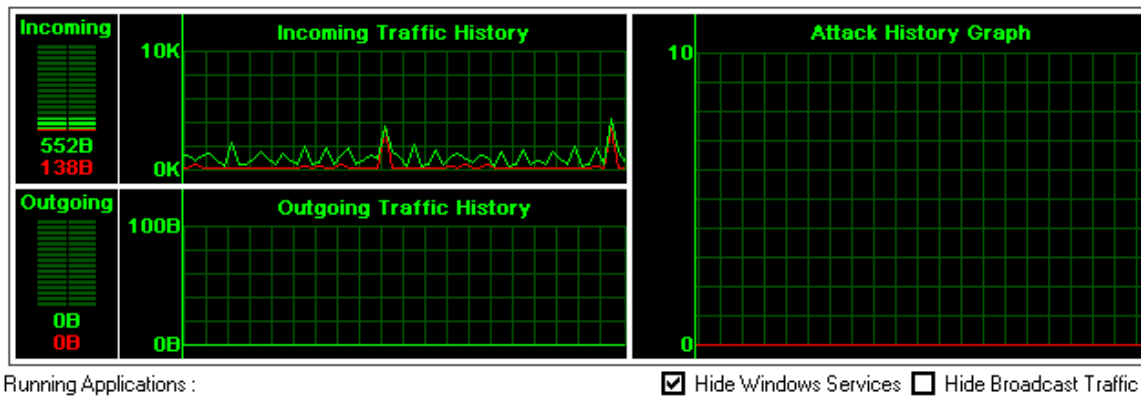


Figure 4. Traffic History Graph

The Traffic History graphs are broken into three sections. On the left side of the graphs section are the Incoming and Outgoing Traffic History graphs. These provide a visual assessment of the current traffic that is entering and leaving your computer through a network interface. This includes traffic that is allowed and traffic that is blocked. The green lines and bars indicate traffic that is allowed to pass through, and the red coloring indicates traffic that is being blocked by the Agent.

Additionally, the Attack History graph on the right side of the console provides information on attempted attacks against your machine.

Broadcast Traffic

Broadcast traffic is network traffic that is sent to every computer in a particular subnet, and thus is not directed specifically to your computer. If you do not want to see this traffic, you can remove it from this graphical view by clicking **Hide Broadcast Traffic** box. You will then only see “unicast” traffic in this graph, which is traffic that directed specifically to your computer. To redisplay broadcast traffic, click to clear **Hide Broadcast Traffic** box.

Running Applications Field




The Running Applications field provides a list of all applications and system services that are currently running on your system.

If you are in client control or power user mode, you may be able to view the access status of the applications. An application’s *access status* refers to the permissions that you allow it. It

shows whether it can access your Internet connection, if it can access that connection without asking you first, or if it is blocked from accessing the Internet or network altogether. If you have a server-controlled Agent, however, you will probably not see any status indications or be able to change the status of an application.

You can change the status of applications from the Running Applications field by right-clicking an application's icon and selecting the desired status.

Table 1. Running Applications Field

Icon	Status	Description
	Allow	Icon appears normal, with no marks
	Ask	Icon appears with a small, yellow question mark
	Block	Icon appears with a red circle and cross-out mark

An application icon displays a small blue dot on lower left-hand or right-hand corner to indicate if it is receiving (left-hand) or sending (right-hand) traffic.



You can hide the display of system services by clicking **Hide Windows Services** above the Running Applications field. There are a number of services running at any given time, and since they are often crucial to the operation of your computer, you most likely want to allow them. If your Agent is client-controlled, you may see pop-ups that ask you if you want to allow these services to run. It is generally fine to allow them, and you can allow them permanently without worry. The Agent blocks the services or applications if anything within the application's executable file changes. For instance, if you download a Trojan horse or an email virus that affects a service or application, the Agent notices the difference and will ask you if you want to allow it. If you have not made any changes to the service or application (such as an upgrade), then you will want to block these applications from running and alert your system administrator.

To change the display of application names, either click the **View** menu, or right-click the Running Applications field and select the desired view.

You can stop an application or service from running by right-clicking the application in the Running Applications field and clicking **Terminate**.

Message Console

The Message Console of the Agent is located below the Running Applications field on the main console. It provides a real-time update of server-client communication, including profile downloads, Profile Serial Numbers, and server connection status.



The Message Console is, by default, hidden.

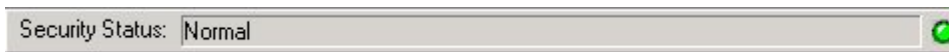
To show or hide the Message Console:

1. Below the Running Applications field, click **Show Message Console**. The Message Console appears.
2. To hide the Message Console from view, click **Hide Message Console**.

The Message Console collapses and displays the **Show Message Console** button.

Status Bar

The Status Bar, located along the bottom of the Agent main console, provides the user with the current location profile information.



Status Light

The status light, in the lower right-hand corner of the main console, gives a real-time update of the Policy Manager-Agent communication status. If green, the light indicates that the Agent is online and communicating with the Policy Manager. If gray, the Agent is not connected to the Policy Manager.

Using the Menus and the Toolbar

The top of the Agent screen displays a standard menu and toolbar. The options vary, depending on the control mode of the Agent:

- Client Control
- Server Control
- Power User Mode

The toolbar buttons located below the menu provide shortcuts that can be used to quickly block all applications, change your application profiles, access the logs, test your Agent using the Sygate Technologies web site, or view the help file.

Menus and Toolbars (Client Control)

The toolbar buttons in Client Control mode can be used to change your application profiles, access the logs, test your Agent using the Sygate Technologies web site, or view the Help file.

If the Agent is operating under Client Control mode, the menu displays the following options: **File**, **Security**, **Tools**, **View**, and **Help**.

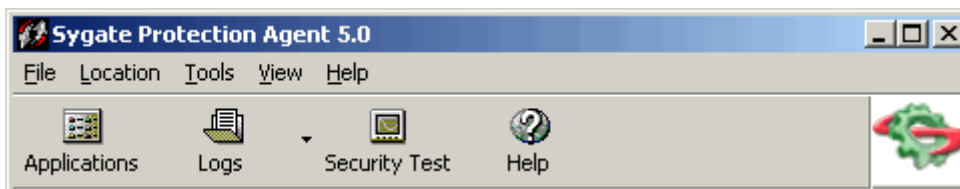


Table 2. Agent Menus (Client Control)

Menu	Menu choices
File	<ul style="list-style-type: none"> • Close—Closes the Agent main console. • Exit Sygate Agent—Closes the Agent, effectively turning off security on your machine. <p>➡ Option Alert: This option may appear dimmed or not at all.</p>
Location	<ul style="list-style-type: none"> • Office—Defines the location for which your Agent is configured. You may have other locations that show, but Office will usually be at least be one of the choices.
Tools	<ul style="list-style-type: none"> • Applications—Opens the Applications List. • Logs—Opens the Logs. • Options—Opens the Options dialog box, which contains many security options, including email alerts, Network Neighborhood browsing rights, and log file configuration. • Advanced Rules—Opens the Advanced Rules dialog box, where you can set very specific rules for the implementation of security on your Agent. • Update Profile—Connects to the Policy Manager immediately to get the latest security policies that have been defined for your Agent. This is normally done on a heartbeat interval. This forces that heartbeat to happen immediately. If you are having difficulty accessing the network, you may need to update your profile by clicking this choice.

Table 2. Agent Menus (Client Control)

Menu	Menu choices
	<ul style="list-style-type: none"> • Update Signature—Not enabled for the Agent. Updates intrusion prevention signatures from the Policy Manager. • Run Host Integrity—Runs a Host Integrity check immediately. If you are in a location where the Sygate Enforcement Agent is disabled, no check will take place. If you are having difficulty accessing the network, you may need to update your Host Integrity status by clicking this choice. If there are no Host Integrity policies defined on the Policy Manager, this option is grayed out. • Automatically Start Service—Not enabled for the Agent. This toggle setting sets whether the Agent will be launched automatically when your machine is booted. • Hide System Tray Icon—This toggle setting hides the system tray icon from view. If it is checked, the icon is hidden. • Test Your System Security—Opens the Sygate Technologies scan site, allowing you to test the effectiveness of the Agent. • Allow All—Allows all network traffic on your machine. • Block All—Blocks all network traffic on your machine.
View	<p>The View menu gives users the option to alter the display of software programs in the Running Applications field:</p> <ul style="list-style-type: none"> • Large Icons—Displays 32x32 icons in the field. Each icon represents a software application or a system service. • Small Icons—Displays 16x16 icons. <p>Both the large and small icon displays provide the full name of the application below the icon itself, and the icons are displayed in a “corkboard” fashion.</p> <ul style="list-style-type: none"> • List—Provides small icon representations, with the icons displayed in a standard list. • Applications Details—Provides not only a list of all running applications, but also useful information on the version number and location path of each application. • Connection Details—Provides further information on the type of connection being made by an each application accessing the network adapter. It also displays the protocol, local and remote ports and IP addresses being used, the application path, and more. • Hide Windows Services—Toggles the display of Windows Services in

Table 2. Agent Menus (Client Control)

Menu	Menu choices
	<p>the Running Applications field.</p> <ul style="list-style-type: none"> • Hide Broadcast Traffic—Toggles the display of broadcast traffic in the Running Applications field.
Help	<ul style="list-style-type: none"> • Help Topics...—Opens the Agent online Help files. • About—Opens the About screen, which tells you the type of Agent that you have as well as more detailed information on the profile and signature files.

Menus and Toolbars (Server Control)

The toolbar buttons in Server Control mode can be used to change your application profiles, access the logs, or view the Help file. Your system administrator may disable some of these buttons.

If the Agent is operating under Server Control mode, the menu displays the following options the following options: **File**, **Location**, **Tools**, **View**, and **Help**.

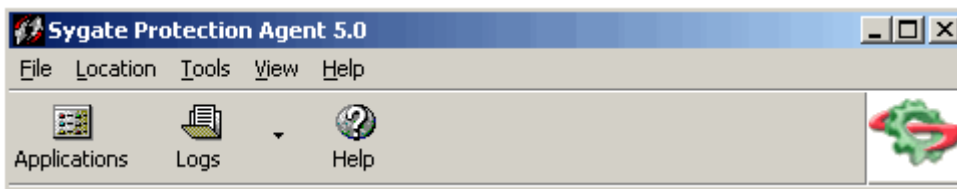


Table 3. Agent Menus (Server Control)

Menu	Menu choices
File	<ul style="list-style-type: none"> • Import Profile—Imports an Agent profile. • Export Profile—Exports an Agent profile. • Close—Closes the Agent main console. • Exit Sygate Protection Agent—Closes the Agent, effectively turning off security on your machine. <p>➡ Option Alert: This option may appear dimmed or not at all.</p>
Location	<ul style="list-style-type: none"> • Office—Defines the location for which your Agent is configured. You may have other locations that show, but Office will at least be one of the choices.

Table 3. Agent Menus (Server Control)

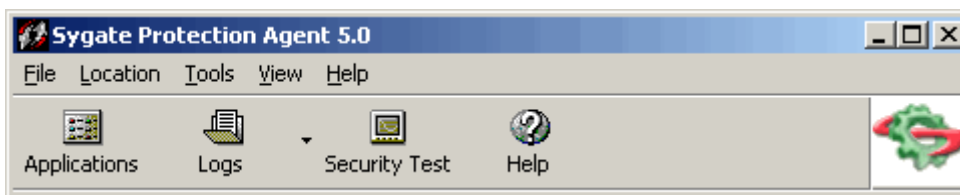
Menu	Menu choices
Tools	<ul style="list-style-type: none"> • Applications—Opens the Applications List. • Logs—Opens Agent Logs. • Update Profile—Connects to the Policy Manager immediately to get the latest security policies that have been defined for your Agent. This is normally done on a heartbeat interval. This forces that heartbeat to happen immediately. If you are having difficulty accessing the network, you may need to update your profile by clicking this choice. • Update Signature—Not enabled for the Agent. Updates intrusion prevention signatures from the Policy Manager.
	<ul style="list-style-type: none"> • Reset Host Integrity Timer—Runs a Host Integrity check immediately. If you are in a location where the Sygate Enforcement Agent is disabled, no check will take place. If you are having difficulty accessing the network, you may need to update your Host Integrity status by clicking this choice. If there are no Host Integrity policies defined on the Policy Manager, this option is grayed out. • Automatically Start Service—Not enabled for the Agent. This toggle setting sets whether the Agent will be launched automatically when your machine is booted. • Hide System Tray Icon—This toggle setting hides the system tray icon from view. If it is checked, the icon is hidden. To show the icon again, click this choice to clear it.
View	<p>The View menu gives users the option to alter the display of software programs in the Running Applications field:</p> <ul style="list-style-type: none"> • Large Icons—Displays 32x32 icons in the field. Each icon represents a software application or a system service. • Small Icons—Displays 16x16 icons. <p>Both the large and small icon displays provide the full name of the application below the icon itself, and the icons are displayed in a “corkboard” fashion.</p> <ul style="list-style-type: none"> • List—Provides small icon representations, with the icons displayed in a standard list. • Applications Details—Provides not only a list of all running applications, but also useful information on the version number and location path of each application.

Table 3. Agent Menus (Server Control)

Menu	Menu choices
	<ul style="list-style-type: none">• Connection Details—Provides further information on the type of connection being made by an each application accessing the network adapter, as well as the protocol, local and remote ports and IP addresses being used, the application path, and more.• Hide Windows Services—Toggles the display of Windows Services in the Running Applications field.• Hide Broadcast Traffic—Toggles the display of broadcast traffic in the Running Applications field.
Help	<ul style="list-style-type: none">• Help Topics...—Opens the Agent online Help files.• About—Opens the About screen, which tells you the type of Agent that you have (Server, Workstation, or AutoLocation Switching), as well as more detailed information on the profile and signature files.

Menus and the Toolbar (Power User Mode)

If the Agent is operating under Power User mode, the menu displays the following options the following options: **File**, **Location**, **Tools**, **View**, and **Help**. This menu is a merging of the options that are available in Client Control and in Server Control, especially in the **Tools** menu.

**Table 4. Agent Menus (Power User)**

Menu	Menu choices
File	<ul style="list-style-type: none">• Import Profile—Imports an Agent profile.• Export Profile—Exports your Agent profile.• Close—Closes the Agent main console.• Exit Sygate Agent—Closes the Agent, effectively turning off security on your machine. ➡ Option Alert: This option may appear dimmed or not at all.

Table 4. Agent Menus (Power User)

Menu	Menu choices
Location	<ul style="list-style-type: none"> • Office—Defines the location for which your Agent is configured. You may have other locations that show, but Office will show for certain.
Tools	<ul style="list-style-type: none"> • Applications—Opens the Applications List. • Logs—Opens Agent Logs. • Options—Opens the Options dialog box, which contains many security options, including email alerts, Network Neighborhood browsing rights, and log file configuration. • Advanced Rules—Opens the Advanced Rules dialog box, where you can set very specific rules for the implementation of security on your Agent. • Security Rule Viewer—This opens the Security Rule Viewer to see the merging of security policies that are represented by Power User Mode. • Update Profile—Connects to the Policy Manager immediately to get the latest security policies that have been defined for your Agent. This is normally done on a heartbeat interval. This forces that heartbeat to happen immediately. If you are having difficulty accessing the network, you may need to update your profile by clicking this choice. • Update Signature—Not enabled for the Agent. Updates intrusion prevention signatures from the Policy Manager. • Run Host Integrity—Resets the timer for evaluating whether your Agent is in compliance with the Host Integrity policies that have been defined by your system administrator, and runs a Host Integrity check immediately. If you are in a location where Host Integrity is disabled, no check will take place. If you are having difficulty accessing the network, you may need to update your Host Integrity status by clicking this choice. If there are no Host Integrity policies defined on the Policy Manager, this option is grayed out. • Automatically Start Service—Not enabled for the Agent. This toggle setting sets whether the Agent will be launched automatically when your machine is booted. • Hide System Tray Icon—This toggle setting hides the system tray icon from view. If it is checked, the icon is hidden. • Test Your System Security—Opens the Sygate Technologies scan site, allowing you to test the effectiveness of the Agent. • Allow All Traffic—Permits all network traffic to flow on your machine. This is almost as non-secure as exiting the Agent, and is not

Table 4. Agent Menus (Power User)

Menu	Menu choices
	<p>recommended.</p> <ul style="list-style-type: none"> • Block All Traffic—Blocks all network traffic on your machine.
View	<p>The View menu gives users the option to alter the display of software programs in the Running Applications field:</p> <ul style="list-style-type: none"> • Large Icons—Displays 32x32 icons in the field. Each icon represents a software application or a system service. • Small Icons—Displays 16x16 icons. <p>Both the large and small icon displays provide the full name of the application below the icon itself, and the icons are displayed in a corkboard fashion.</p> <ul style="list-style-type: none"> • List—Provides small icon representations, with the icons displayed in a standard list. • Applications Details—Provides not only a list of all running applications, but also useful information on the version number and location path of each application. • Connection Details—Provides further information on the type of connection being made by an each application accessing the network adapter, as well as the protocol, local and remote ports and IP addresses being used, the application path, and more. • Hide Windows Services—Toggles the display of Windows Services in the Running Applications field. • Hide Broadcast Traffic—Toggles the display of broadcast traffic in the Running Applications field.
Help	<ul style="list-style-type: none"> • Help Topics...—Opens the Agent online Help files. • About—Opens the About screen, which tells you the type of Agent that you have (XP Embedded, Server, Workstation, or AutoLocation Switching), as well as more detailed information on the profile and signature files.

Using the System Tray Icon

Once installed, the Agent displays a small icon in your system tray (located on the right-hand side of your taskbar). You can double-click to open the Agent or right-click to see a menu of commands.



The icon consists of two arrows that represent system traffic: the upward-pointing arrow is outgoing traffic; the downward-pointing arrow is incoming traffic.

These arrows give you a real-time update of your computer's traffic flow. You might not see a constant icon appearance for more than a few seconds, especially if you frequently use the Internet or your network connection.

What the System Tray Icon Tells You

The colors of the arrows are always changing (as is the traffic flow on your computer). For most users, it should be sufficient to remember the following points about the colors of the icon.

Table 5. System Tray Icon Colors

If the color of the arrow is	- then -
RED	traffic is being blocked by the Agent.
BLUE	traffic is flowing uninterrupted by the Agent.
GRAY	no traffic is flowing in that direction.
GRAY with green dot	no traffic is flowing, but Agent is connected to Policy Manager.

The following table illustrates the different appearances that the system tray icon may have, and what they mean.

Table 6. System Tray Icon Appearance



Icon	Description
	The Agent is in Alert Mode. This means that an attempted attack against your computer has been recorded in your Security Log. To make the icon stop flashing, double-click the icon. The Security Log will open, displaying a new log entry.
	The Agent is in Allow All mode.

Table 6. System Tray Icon Appearance

Icon	Description
	The Agent is in Block All mode.
	Incoming traffic is flowing uninterrupted; there is no outgoing traffic.
	Both incoming and outgoing traffic are flowing uninterrupted.
	There is no incoming traffic; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; there is no outgoing traffic.
	Both incoming and outgoing traffic are blocked
	There is no incoming traffic; outgoing traffic is blocked.
	Incoming traffic is flowing uninterrupted; outgoing traffic is blocked.
	No traffic is flowing in either direction.
	Both incoming and outgoing traffic flows uninterrupted; the Agent is disabled.

What Does the Flashing System Tray Icon Mean?

The system tray icon sometimes flashes on and off. This means that the Agent is in Alert mode, which is caused by one of the following:

- An attack has been recorded on your computer in the Security Log.
- You are missing a file or an application that is required by your system administrator before you can log into the network. If a file or an application is missing, a message is probably displayed that lists the missing files, or, applications that you need to install before you can proceed. If a system administrator does not configure the Agent to display certain types of messages, then no notification occurs.

If the reason for the flashing is an attack, you can open the Security Log. This stops the icon from flashing. Otherwise, the icon keeps flashing and you need to ask your system administrator to install any missing files or applications.

The System Tray Icon Menu

You can easily configure basic aspects of the Agent without even opening the main console. You can right click the system tray icon to display a menu. What you see on this menu is dependent upon the control mode of your Agent. You can roll your mouse over the system tray icon to see your current location, host integrity status, and connection status.

The system tray icon includes the following right-click commands.

Table 7. System Tray Icon Menu

Server Control	Client Control	Power User	Menu Option	Description
X	X	X	Sygate Protection Agent	Opens the Agent's main console.
X	X	X	Location	Opens the Location List. You can change locations if your security settings permit.
X	X	X	Applications	Opens the Applications list.
X	X	X	Logs	Opens the Agent logs.
	X	X	Options...	Opens the Options dialog box, where you can configure the settings for the Agent.
	X	X	Advanced Rules	Opens the Advanced Rules dialog box, where you can write specific rules for allowing or blocking network access.

Table 7. System Tray Icon Menu

Server Control	Client Control	Power User	Menu Option	Description
X	X	X	Run Host Integrity	Causes a Host Integrity check to begin immediately. This will ensure that your Agent is running the latest security policies and has the latest software patches, antivirus definitions, and so on, that have been defined on the Management Server. If you are in a location where Host Integrity is disabled, no check will take place.
X	X	X	Hide System Tray Icon	<p>Removes the system tray icon from the taskbar. The Agent is still running.</p> <p>To redisplay the icon, on the Start menu, click Programs Sygate Protection Agent. Then, from the Tools menu, click the Hide System Tray Icon to toggle the choice back on.</p>
X	X	X	Help Topics...	Opens the online Help system.
X	X	X	About...	Opens the About dialog box, providing information on your version of the Agent.
X	X	X	Exit Sygate Protection Agent	<p>Stops the Agent from running. You need to restart the Agent to protect your system.</p> <p>➡ Option Alert: This option may appear dimmed or not at all.</p>

Hiding and Displaying the System Tray Icon

There are several ways to hide and redisplay the system tray icon on the taskbar.

➡ **Option Alert:** This option may not be available in your control mode.

To hide the system tray icon:

- Right-click the system tray icon and click **Hide System Tray Icon**.
- Click **Tools | Hide System Tray Icon**.

To display the system tray icon:

- Click **Tools | Hide System Tray Icon**.

Changing Locations

Locations are defined in the Policy Manager by your system administrator. Your administrator can use Locations to define different security levels based on your physical location when you try to connect to the network. For example, if you connect to the office network using your laptop from home, your system administrator can set up a location named Home. If you are using the laptop in the office, then you may use a location named Office. Other locations could include VPN, a branch office, or hotel. Each of these locations can have different security policies. Actions that you can perform when you are located in the office, might not be allowed when you are connecting from a hotel. Your system administrator has planned and configured locations and your Agent will most likely detect these changes and automatically switch when you connect.

Depending on the profiles that have been set up for you, you may or may not have more than one location available under the menu. You may find that when you click a location, you do not change to that location. This means that your network configuration is not appropriate for that location. For example, if you have a location called Office, it may be configured to use this location only when it detects the office Local Area Network. If you are not currently on that network, you cannot change to that location.

To change your location:

1. Do one of the following:
 - On the main console, click the **Location** menu.
 - Right-click the system tray icon, and click **Location**.
2. Click one of the listed locations.

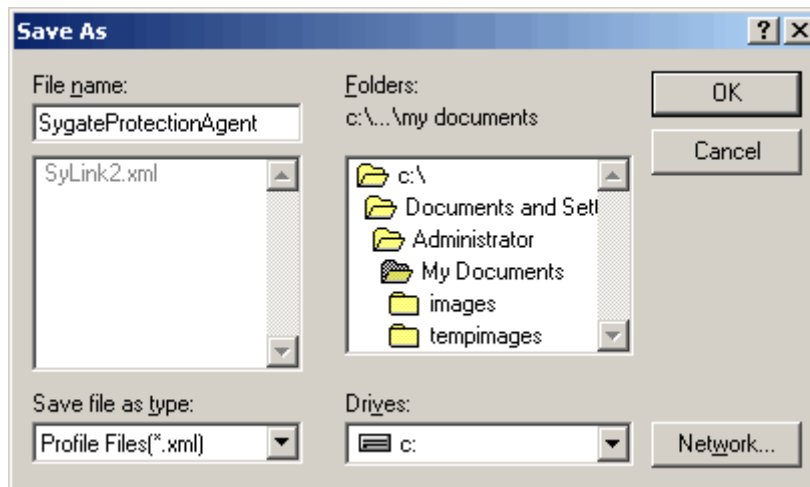
Importing and Exporting Profiles

Profiles can be imported and exported from the Agent console. Your system administrator may request that you do this, but otherwise it is unlikely that you will need to do it.

➡ **Option Alert:** This option is available in Server Control and Power User modes only.

To export profiles from the main console:

1. On the **File** menu, click **Export Profile**.
2. The Save As dialog box opens. Browse to find the appropriate folder for the file, and enter a file name.



3. Click **OK**. The file is saved as an XML file in the designated location.

To import profiles to the main console:

1. On the **File** menu, click **Import Profile**.
2. The Open dialog box opens. Browse to find the appropriate file.
3. Click **OK**. The profile is applied to the Agent.

Using the Security Rule Viewer

The **Security Rule Viewer** (the Rule Viewer) is your key to understanding which security policies are in effect on your computer. It shows you the rules that the Policy Manager has placed on your computer and the rules and security settings that you have created yourself. These are all presented in a single viewer that shows each rule or setting, a description of that rule or setting, and the action (usually Allow or Block) that the rule causes.

➡ **Option Alert:** This option is available in Power User mode only.

Order of Priority of Agent versus Policy Manager Rules

The order of priority:

1. **Server Rules with high priority levels** as assigned by the system administrator
2. **Agent Advanced Rules**
3. **Server Rules with lower priority levels**
4. **Agent Network Neighborhood** Settings
5. **Agent Application** Settings

How the Security Rule Viewer Works

The Security Rule Viewer provides you with an integrated view of the security rules and settings that are running on your Agent. When you click on a Server rule, a summary of that rule appears in the summary box at the bottom of the screen. Clicking on an Agent rule takes you directly to the Applications List, the Configuration Options dialog box, or the Advanced Rule Settings dialog box, where you can fine-tune the rule.

Chapter 4. Protecting Your System

If your Agent is in Server Control mode, your system administrator has set your security settings. You do not have access to the security settings from your Agent software. However, when in Client Control or Power User mode, you can access certain settings. You can set:

- Access status for applications
- Advanced application configuration
- General configuration settings
- Advanced rules

You set application access using the applications list, you can set each application's status to Allow, Ask, or Block. Allow status gives an application full access, Ask status requires your intervention to determine status, Block status completely blocks the application.

From the Application window, you can use the Advanced button to configure advanced application settings. These settings include trusted IP addresses, ports, and scheduling.

You can set general configuration settings using Options from the Tools Menu. Here you can set items such as email notification, log settings, and IEEE authentication.

Using Advanced rules, you can configure rules that override the rules automatically created by the firewall during normal user-firewall interaction and the rules you set up for individual applications. Advanced rules affect all applications.

You can test your system's vulnerability by using the scanning feature. Scanning can help you determine the types of security for your system.

If your Agent is in Server Control mode, your system administrator has set your security settings. You do not have access to the security settings from your Agent software. However, when in Client Control or Power User mode, you can access certain settings. You can set:

- Access status for applications

- Advanced application configuration
- General configuration settings
- Advanced rules

You set application access using the applications list, you can set each application's status to Allow, Ask, or Block. Allow status gives an application full access, Ask status requires your intervention to determine status, Block status completely blocks the application.

From the Application window, you can use the Advanced button to configure advanced application settings. These settings include trusted IP addresses, ports, and scheduling.

You can set general configuration settings using Options from the Tools Menu. Here you can set items such as email notification, log settings, and IEEE authentication.

Using Advanced rules, you can configure rules that override the rules automatically created by the firewall during normal user-firewall interaction and the rules you set up for individual applications. Advanced rules affect all applications.

You can test your system's vulnerability by using the scanning feature. Scanning can help you determine the types of security for your system.

Scanning Your System

Assessing your vulnerability to an attack is one of the most important steps that you can take to ensure that your system is protected from possible intruders. With what you learn from this battery of tests, you can more effectively set the various options on your Agent to protect your system from attack.

To scan your system:

1. Do one of the following:
 - On the toolbar, click the **Security Test** button.



- On the **Tools** menu, click **Test Your System Security**.
 - In your Internet browser window, open the Sygate Technologies web page (<http://scan.sygate.com>) directly.
1. On the web page, click **Scan Now**. The Sygate Online Services scanner scans your computer and attempts to determine your IP address, operating system, web browser, and other information about your system.
 2. For information on a specific type of scan, click one of the following:

- Quick Scan
- Stealth Scan
- Trojan Scan
- TCP Scan
- UDP Scan
- ICMP Scan

4. Click **Scan Now**.

A brief document of frequently asked questions about Sygate Online Services is also available from the main scan page. Click **Scan FAQ** at the bottom left side of the screen.

Types of Scans

On the Sygate Technologies web site, you can choose from one of the following types of scans.

Quick Scans

The Quick Scan is a brief, general scan that encompasses several scanning processes. It usually takes 20 seconds or less to accurately scan your computer's ports, protocols, services, and possible Trojans. The results are recorded in the Agent's Security Log.

Stealth Scans

The Stealth scan scans your computer using specialized stealthing techniques, which mimic portions of legitimate computer communication to detect the presence of a computer. The Stealth scan takes about 20 seconds to complete and is most likely not recorded in the Security Log.

Trojan Scans

The Trojan scan feature scans all of your computer's 65,535 ports for active Trojan horse programs that you or someone else may have inadvertently downloaded. The Trojan scan takes about 10 minutes to complete. A list of common Trojans is available on the web site.

TCP Scans

The TCP scan examines the 1,024 ports that are mainly reserved for TCP services, such as instant messaging services, to see if these ports are open to communication. Open ports can indicate a dangerous security hole that can be exploited by malicious hackers.

It scans ports on your computer that are connected to devices such as routers and proxies for users connecting to the web site through such a device. The scan takes about 20 minutes to complete and is logged by the Agent as a scan event in the Security Log.

UDP Scans

The UDP scan uses various methods and protocols to probe for open ports utilizing UDP. The UDP scan will scan ports on your computer that are connected to devices such as routers and proxies for users connecting to the web site through such a device. The scan takes about 10 minutes and should be logged in the Security Log as a port scan from Sygate.

ICMP Scans

When an ICMP scan has completed scanning a user's computer, it displays a page with the results of the scan. If a user is running the Agent, all scans are blocked.

Setting the Access for Applications

➡ **Option Alert:** This option is available in the Client Control and Power User Mode only.

You can set an access status (**Allow/Block/Ask**) for each application or service, such as Internet Explorer, that tries to gain access through your network connection.

The access status types are:

- **Allow:** The Agent allows incoming and outgoing traffic to access network. This is usually traffic that is known to be “safe,” either because you are in Server Control and your system administrator has defined it to be safe, or because you are in Client Control and you have made that determination yourself. A application can also be configured to access the network only if using a certain port, or during certain hours.
- **Ask:** When a new application attempts to access your network connection while you are under the default setting (Normal), the Agent displays a pop-up window to ask if you want to allow the application to access the network. If you have not allowed or blocked an application, the Agent prompts you every time it tries to gain access to the network or modem. You can also tell it to remember your response for future access attempts by the same application.
- **Block:** The Agent denies incoming and outgoing traffic. If you are in Server Control, your system administrator has already created rules that block your computer.

To change the access status of an application:

1. Do one of the following:
 - Click the **Applications** icon on the toolbar.
 - Click **Tools | Applications**.

- Right-click the system tray icon and click **Applications**.

The **Applications** dialog box displays all applications and services that have asked you for permission to access your network connection since the installation of the Agent. Some applications may have already been pre-approved by your system administrator, and do not appear in this dialog box.

2. Click the file name of the appropriate application so that the row is highlighted.
3. Right-click the highlighted row.
4. Click the appropriate access status (**Allow**, **Ask**, or **Block**) from the shortcut menu.
5. Click **OK** to close the Applications dialog box.

Note: You can remove selected or all applications from the list by clicking the **Remove** or **Remove All** button. Once an application/service is removed from the Applications List, its status is erased. When that application/service attempts to connect to the network again, you will get a pop-up message and be asked to assign a new status to the application/service.

You can change the display view for the applications and services by right-clicking the Applications dialog box, clicking **View**, and clicking the desired view.

Setting Advanced Options for Applications

You can set the access permissions for your applications using the Applications List. The Applications List shows all applications and services that have asked you for permission to access your network connection since the installation of the Agent software. The application/service name, version, status, and path are provided in a simple screen. Some applications (such as Internet Explorer) may have already been pre-approved by your system administrator, and will thus not appear in this window.

To open the Applications List do one of the following:

- Click the **Applications** icon on the toolbar.
- Click **Tools | Applications**.
- Right-click the system tray icon and click **Applications**.

To select an application or service for configuration, click on any of its attributes as shown in the Applications List. The application or service name must be highlighted before you can change or configure its status.

The buttons at the bottom of the Applications List screen provide the option to remove selected or all applications from the list. Once an application/service is removed from the Applications List, its status is erased. When that application/service attempts to connect to

the network again, you will be notified through a new application pop-up message and be asked to assign a new status to the application/service.

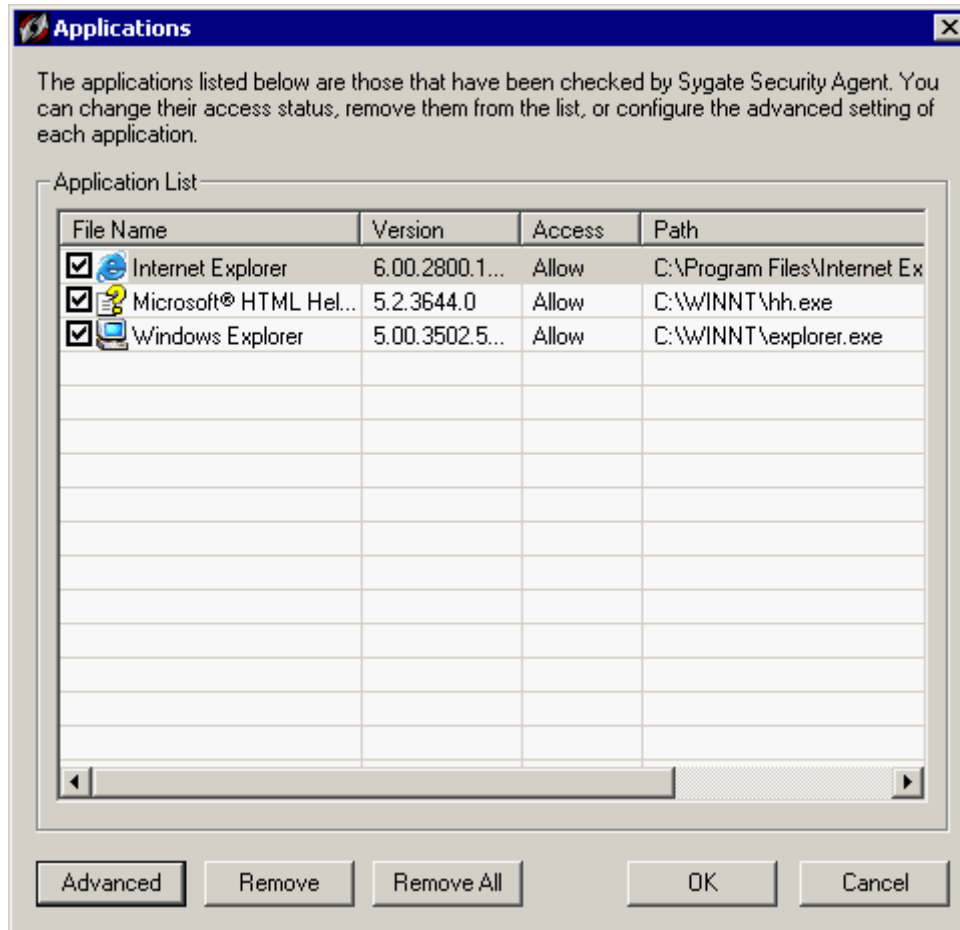


Figure 6. Applications List

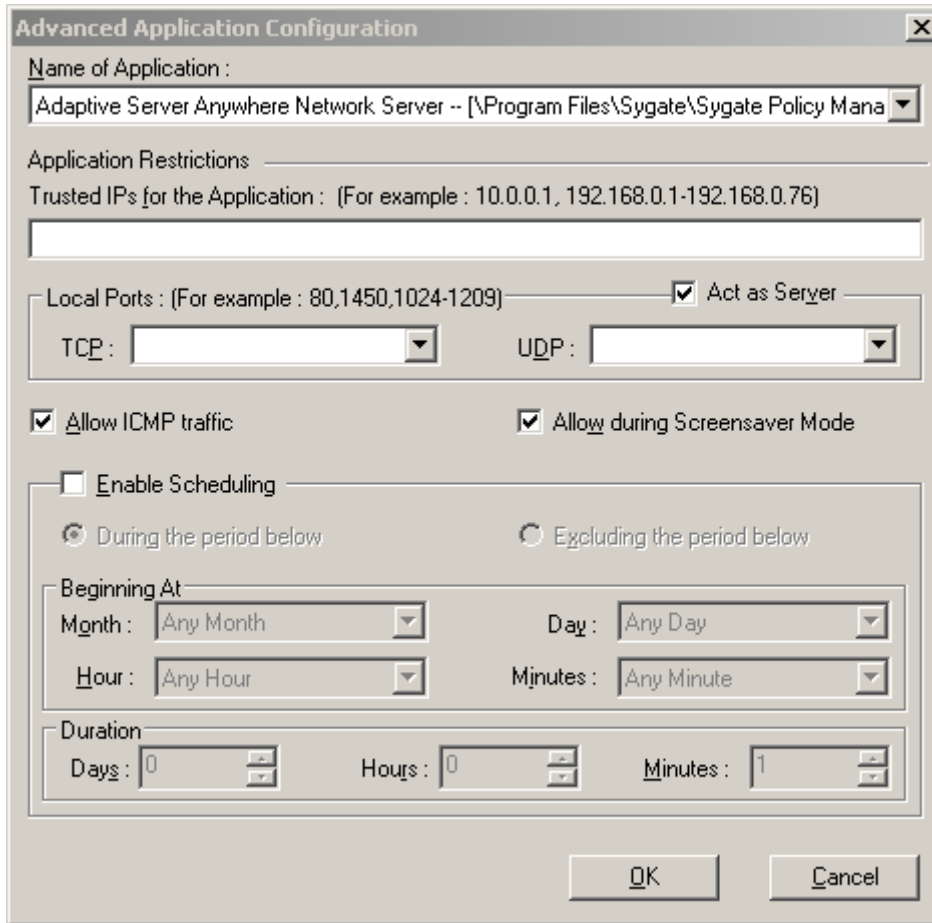
Advanced Application Configuration (Client Control, Power User Mode)

You can configure advanced security settings for each application on your application list. You do this by setting certain restrictions on the IP addresses and ports an application can utilize. Only users who have a firm grasp on computer ports and application protocols should use the advanced configuration options.

To Set Up Advanced Configuration:

1. Open the Applications List.
2. Make sure that the correct application is selected in the Name of Application list box.
3. Click the **Advanced** button at the bottom left corner of the Applications List screen.

4. The Advanced Application Configuration dialog box opens. You can now set the options for this application.



The image shows the 'Advanced Application Configuration' dialog box. It has a title bar with a close button. The main area contains several sections: 'Name of Application' with a dropdown menu showing 'Adaptive Server Anywhere Network Server -- (\Program Files\Sygate\Sygate Policy Mana...'; 'Application Restrictions' with a text box for 'Trusted IPs for the Application' and a hint '(For example : 10.0.0.1, 192.168.0.1-192.168.0.76)'; 'Local Ports' with dropdowns for 'TCP' and 'UDP' and a checked 'Act as Server' checkbox; 'Allow ICMP traffic' and 'Allow during Screensaver Mode' checkboxes; 'Enable Scheduling' with radio buttons for 'During the period below' and 'Excluding the period below'; 'Beginning At' with dropdowns for 'Month', 'Day', 'Hour', and 'Minutes'; and 'Duration' with spinners for 'Days', 'Hours', and 'Minutes'. At the bottom are 'OK' and 'Cancel' buttons.

Figure 7. Advanced Application Configuration

Application Restrictions: Enter trusted IPs or IP ranges in the Trusted IPs for the Application text box.

Local Ports: Enter the ports or ranges of ports that can be utilized for this application.

Allow ICMP Traffic: Outgoing ICMP echo-request (type:8, code:0) and incoming ICMP echo-reply (type:0, code:0) will always be allowed.

Allow during Screensaver Mode: Decide if the application should be allowed network access during Screensaver Mode.

Enable Scheduling: Select this option if you wish to set a time limit or schedule specific periods when the restrictions will be in effect.

You can set the time the advanced configurations takes effect. This scheduling lets you set up the application restrictions to be in effect either *during* a specific time period, or *excluding* a specific time period.

Configuring the Agent's Settings

You can set and import advanced security options for the Agent, including e-mail notification of attacks, customizable pop-up messages, heartbeat settings, log file configuration, file sharing options, computer control settings, and advanced security measures such as Smart DHCP and Anti-MAC spoofing.

➡ **Option Alert:** This option is available for the Client Control and Power User Mode only.

To configure the Agent do one of the following:

- On the **Tools** menu, click **Options**.
- Right-click the system tray icon and click **Options**.
- In any log, on the **File** menu, click **Options**.

The Options dialog box consists of the following tabs:

- General tab
- Network Neighborhood tab
- Security tab
- E-Mail Notification tab
- Log tab
- IEEE 802.1x Authentication

You can set and import advanced security options for the Agent, including e-mail notification of attacks, customizable pop-up messages, heartbeat settings, log file configuration, file sharing options, computer control settings, and advanced security measures such as Smart DHCP and Anti-MAC spoofing.

➡ **Option Alert:** This option is available for the Client Control and Power User Mode only.

To configure the Agent do one of the following:

- On the **Tools** menu, click **Options**.
- Right-click the system tray icon and click **Options**.
- In any log, on the **File** menu, click **Options**.

The Options dialog box consists of the following tabs:

- General tab
- Network Neighborhood tab
- Security tab
- E-Mail Notification tab
- Log tab
- IEEE 802.1x Authentication

General Tab

The **General** tab includes some of the more broad and global settings.

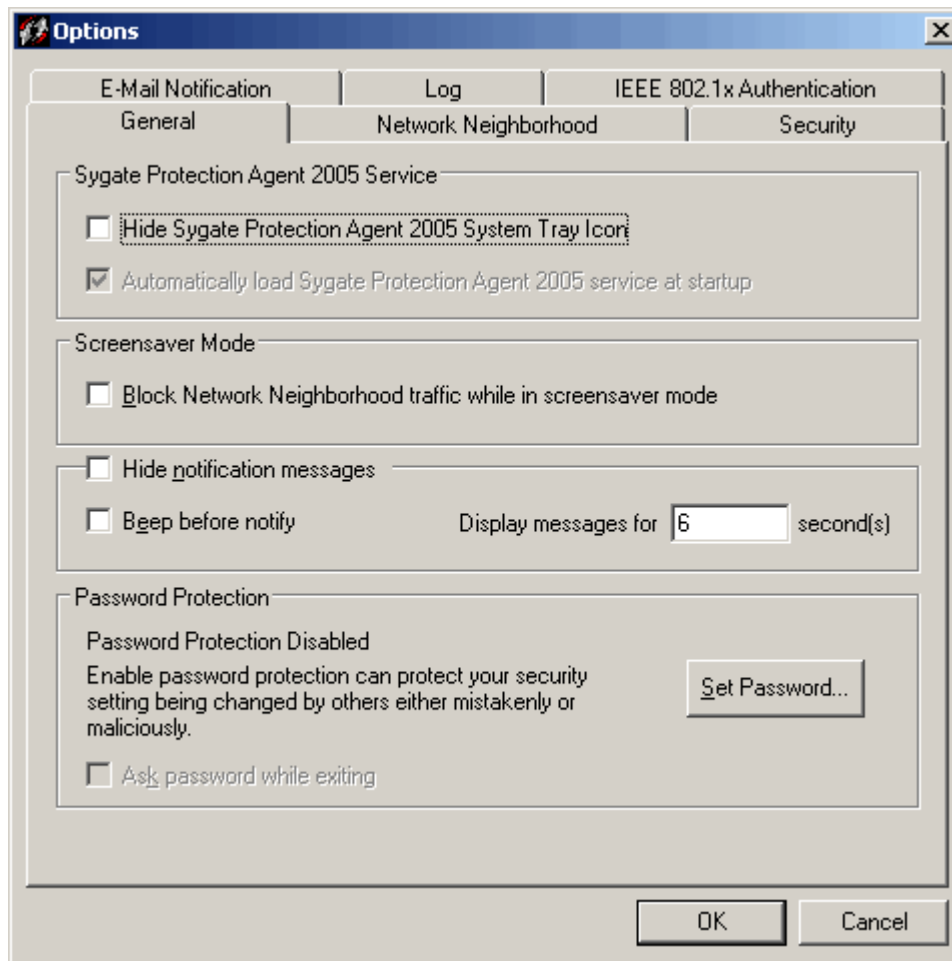


Figure 8. Options: General Tab

Hide Sygate Protection Agent System Tray Icon

Hides the icon from view on the taskbar. To redisplay, click to clear this check box.

Automatically load Sygate Security Agent at startup

Automatically launches the Agent at startup.

Block Network Neighborhood traffic while in screensaver mode

Automatically sets your security level to **Block All** when your computer's screensaver is activated. As soon as the computer is used again, the security level returns to the previously assigned level.

Hide notification messages

Disables the system tray notification messages. By default, this option is not checked.


Beep before notify

Allows audio announcement first before system tray notification messages appear.

Display messages for __ seconds

Allows you to set the duration that messages will display. The default is 6 seconds.

Set Password

 **Option Alert:** This option is available in Client Control and Power User mode only.

Opens the Password dialog box so that you can set password protection on the Agent. This prohibits other users from accessing your Agent and possibly changing your settings. If enabled, password protection prompts for a password every time the Agent's main console is accessed.

You can set your Agent to require a password prior to making any security changes, and to require a password before exiting the Agent.

To enable password protection:

1. Click the **Tools | Options | General** tab.
2. Click the **Set Password...** button at the bottom right of the dialog box. The following **Password** dialog box appears.



3. Enter your new password in the **New Password** and **Confirm New Password** fields.

Note: You can disable password protection by leaving the **New Password** and the **Confirm New Password** fields blank.

4. To have the Agent prompt you for a password before exiting the Agent, on the **General** tab, click **Ask password while exiting**.
5. Click **OK** to confirm or click **Cancel** to discard your changes.

Ask password while exiting

Prompts you to enter your password when closing the Agent.

Network Neighborhood Tab

The **Network Neighborhood** tab provides multiple interface support and network browsing rights configuration.

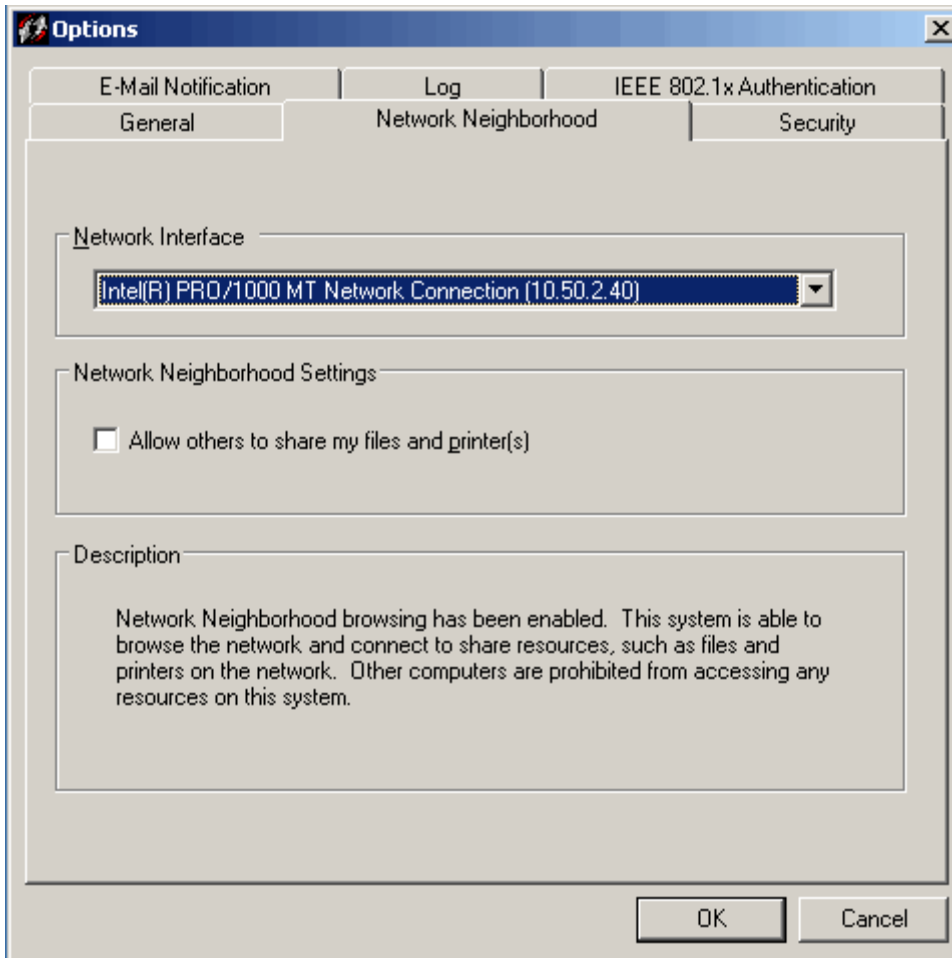


Figure 9. Options: Network Neighborhood Tab

Network Interface

Specifies the network you want to access.

Allow others to share my files and printer(s)

Allows other users of the selected network to browse your computer and printer(s).

Security Tab

The **Security** tab offers a way to enable and disable some of the more complex security options. You should test settings made here before propagating them to other computers to make certain that they work as intended.

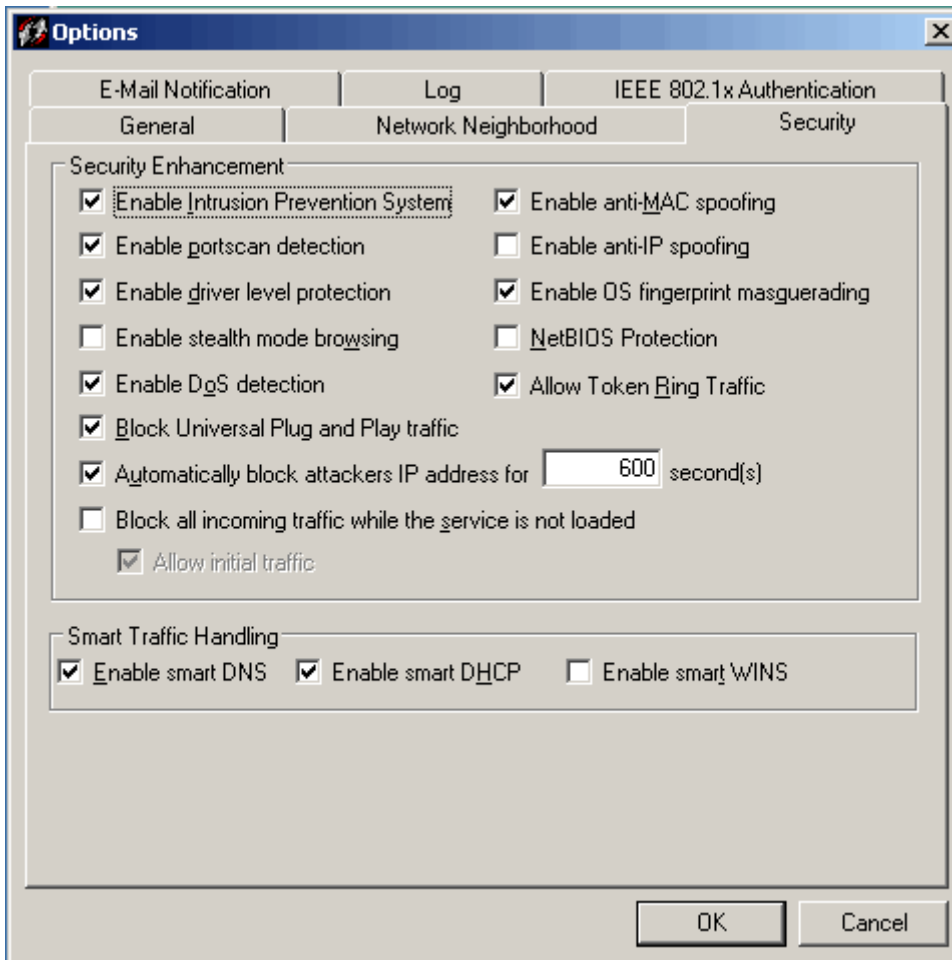


Figure 10. Options: Security Tab

Enable Intrusion Prevention System

Provides you with alerts when another user attempts to compromise your system. Intrusion prevention on the Agent actually enables a combination of both an intrusion detection system (IDS) and an intrusion prevention system (IPS). The end result is a system that analyzes network packets and compares them with both known attacks and known patterns of attack, and then blocks those attacks. One of the key capabilities of the Intrusion Prevention System is its capability to do deep packet inspection. By default, this option is enabled on the Agent.

Enable port scan detection

Detects if someone is scanning your ports, and notifies you. Port scanning is a popular method that hackers use to determine which of your computer ports are open to communication. Ports are dynamically blocked by the Agent and are therefore protected from hacking attempts.

If disabled, the Agent does not detect scans or notify you of them, but still protects your ports from hacking attempts. By default, this option is enabled on the Agent.

Enable driver level protection

Blocks protocol drivers from accessing the network unless the user gives permission. If a protocol driver attempts to access the network, you will see a pop-up message asking if you want to allow it. By default, this option is already enabled.

Enable stealth mode browsing

Stealth mode describes a computer that is hidden from web servers while on a network. A computer on the Internet, for instance, if in stealth mode, cannot be detected by port scans or communication attempts, such as **ping**. By default, this option is disabled.

Enable DoS detection

Causes the Agent to check incoming traffic for known Denial of Service (DoS) attack patterns. DoS attacks are characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service. By default, this option is enabled.

Block Universal Plug and Play Traffic

Causes the Agent to look for and block UPnP traffic to counter the vulnerabilities that are introduced by this operating system feature: The first vulnerability could enable an attacker to gain complete control over an affected system, while the second vulnerability could enable an attacker to either prevent an affected system from providing useful service, or utilize multiple users' systems in a distributed denial of service attack against a single target. Users can disable this feature when using applications that require the UPnP protocol to operate. By default, this option is enabled.

Automatically block attacker's IP address for... second(s)

Blocks all communication from a source host once an attack has been detected. For instance, if the Agent detects a DoS attack originating from a certain IP address, the Agent will block any and all traffic from that IP for the duration specified in the seconds field. By default, this option is enabled.

Block all incoming traffic while the service is not loaded

Prevents any traffic from entering or leaving your computer during the seconds between the time that your machine turns on and the Agent is launched. This time frame is a small security hole that can allow unauthorized communication. Enabling this feature prevents possible Trojan horses or other unauthorized applications from communicating with other computers or devices. This also takes effect if the Agent crashes or if the Agent is shut down. By default, this option is enabled.

Allow initial traffic

Enables initial traffic needed for basic network connectivity. This includes initial DHCP and NetBIOS traffic so that the Agent can obtain an IP address. By default, this option is enabled.

Enable anti-MAC spoofing

Allows incoming and outgoing Address Resolution Protocol (ARP) traffic only if an ARP request was made to that specific host. It blocks all other unexpected ARP traffic and logs it in the Security Log. By default, this option is enabled on the Agent.

Some hackers use MAC spoofing to attempt to hijack a communication session between two computers in order to hack one of the machines. MAC (media access control) addresses are hardware addresses that identify computers, devices, servers, routers, etc. When Computer A wants to communicate with Computer B, it may send an ARP packet to the computer.

Enable anti-IP spoofing

IP spoofing is a process used by hackers to hijack a communication session between two computers. For example, if you have computers A and B, a hacker can send a data packet that causes Computer A to drop the communication. Then, pretending to be Computer A, the hacker can communicate with Computer B, thus, hijacking a communication session and attempting to attack Computer B.

Anti-IP spoofing foils most IP spoofing attempts by randomizing the sequence numbers of each communication packet, preventing a hacker from anticipating a packet and intercepting it. It is recommended that you enable this option along with **Enable OS fingerprint masquerading**. By default, this option is enabled.

Enable OS fingerprint masquerading

Keeps programs from detecting the operating system of a computer running the Agent software. When OS Fingerprint Masquerading is enabled, the Agent modifies TCP/IP packets so it is not possible to determine its operating system. It is recommended that you enable this option along with **Enable anti-IP spoofing**, discussed previously. By default, this option is enabled.

NetBIOS protection

Blocks all communication from computers located outside the Agent's local subnet range. NetBIOS traffic is blocked on UDP ports 88, 137, and 138 and TCP ports 135, 139, 445, and 1026. Be aware that this can cause a problem with Outlook if connecting to an Exchange server that is on a different subnet. If that occurs, you should create an advanced rule specifically allowing access to that server.

Allow Token Ring Traffic

Allows Agents connecting through a token ring adapter to access the corporate network. By default, this option is enabled.

Enable smart DNS

Blocks all DNS traffic except for outgoing DNS requests and the corresponding replies. This means that if your computer sends out a DNS request, and another computer responds within five seconds, the communication will be allowed. All other DNS packets will be dropped.

If you disable this feature, please note that you will need to manually allow DNS name resolution by creating an advanced rule that allows UDP traffic for remote port 53. By default, this option is enabled.

Enable smart DHCP

Allows only outgoing DHCP requests and incoming DHCP replies, and only for network cards that allow DHCP.

If you disable this feature and need to use DHCP, you must create an advanced rule for UDP packets on remote ports 67 and 68. By default, this option is enabled.

Enable smart WINS

Allows Windows Internet Naming Service (WINS) requests only if they were solicited. If the traffic was not requested, the WINS reply is blocked. By default, this option is disabled.

E-Mail Notification Tab

The **E-Mail Notification** tab provides you with the option to automatically notify a specified recipient through an e-mail message of any attacks against your computer.

Note: It is important that you always use the Test E-Mail Notification button after entering email addresses to verify the addresses you entered are correct.

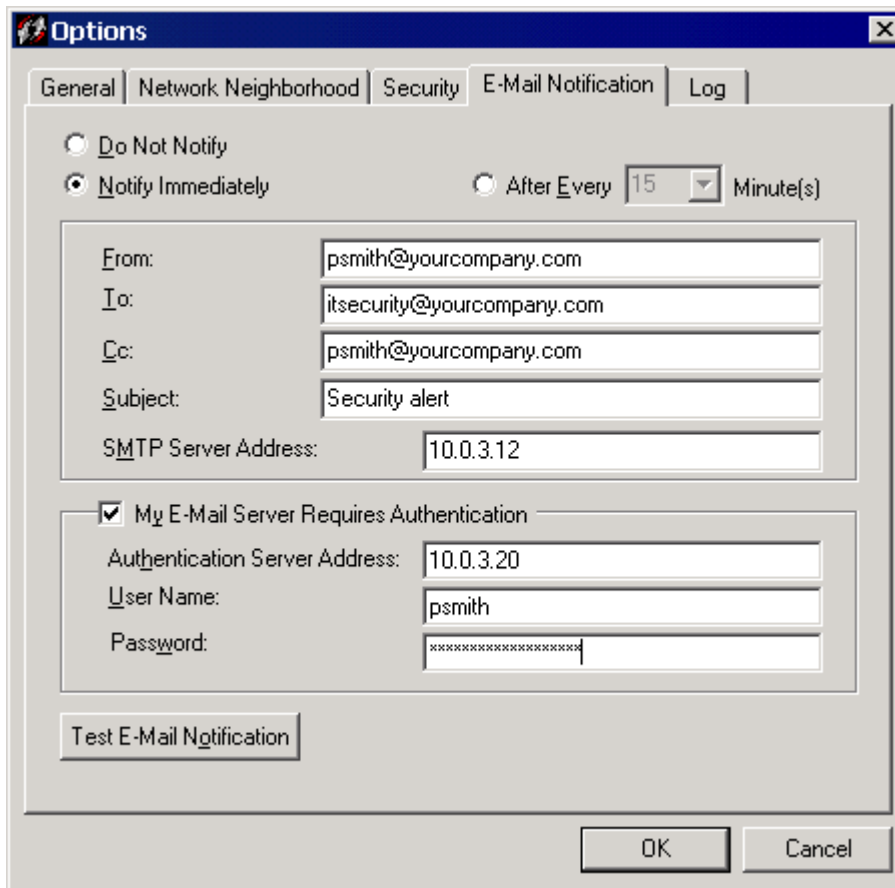


Figure 11. Options: E-Mail Notification Tab

The first three options set the frequency of the message.

Do Not Notify

Disables the e-mail notification option.

Notify Immediately

Sends an e-mail message immediately following an attack on your computer.

After Every __ Minutes

Sends an e-mail message at regular intervals following an attack, the intervals specified in the **After Every __ Minute(s)** dial.

From:

Specifies an e-mail address for the person sending the message. This can be your personal e-mail address, or another e-mail address.

To:

Specifies a recipient e-mail address. This can be an administrator's email address, or any other e-mail address.

Cc:

Specifies an e-mail address to send a courtesy copy of each email message.

Subject:

Describes the subject of the e-mail message.

SMTP Server Address:

Specifies your SMTP Server Address.

My E-Mail Server Requires Authentication

Specifies whether your e-mail server requires authentication.

Authentication Server Address:

Specifies the address of the authentication server.

User Name/Password:

Specifies your username and password for the authentication server in the appropriate fields.

Test E-Mail Notification

Sends a test message to the e-mail address that you specified in the **To:** and **CC:** fields.

It is important that you use the test button to verify any email address you input.

Log Tab

The **Log** tab provides a central location to manage the logs for the Agent. You can determine the standard log size for each log, as well as specify how many days of entries are recorded in each log. You can also toggle whether or not logs are kept for each type of log.

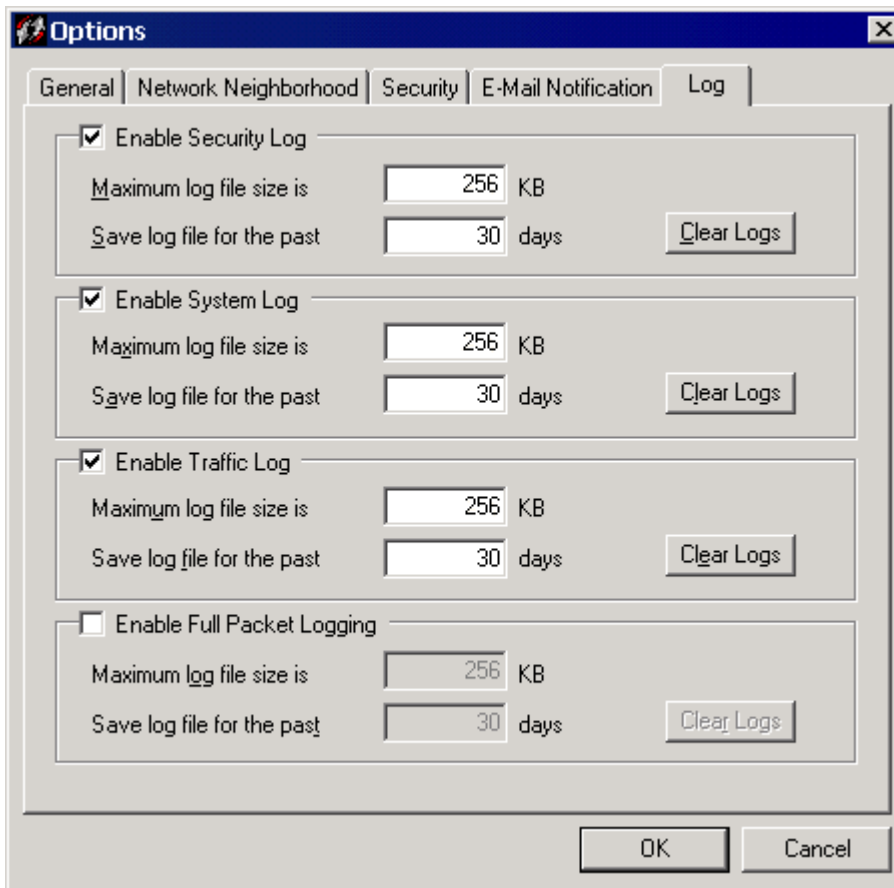


Figure 12. Options: Log Tab

Enable Log

Enables the Security, Traffic, System, and Packet Logs. The Packet Log is not enabled by default.

Maximum log file size

Specifies the maximum size for the log file in kilobytes. The default setting is either 512 KB or 1024 KB. It is recommended that the log file size is kept as small as possible.

Save log file for the past xx days

For the log you want to configure, specifies the number of days to save the log.

Clear Logs

Clears the selected log.

IEEE 802.1x Authentication Tab

The **IEEE 802.1x Authentication** tab is used if your corporation enforces 802.1x or EAP Authentication with a LAN Enforcer when connecting to the corporate network.

➡ **Option Alert:** The IEEE 802.1x Authentication tab is available in Client Control only.

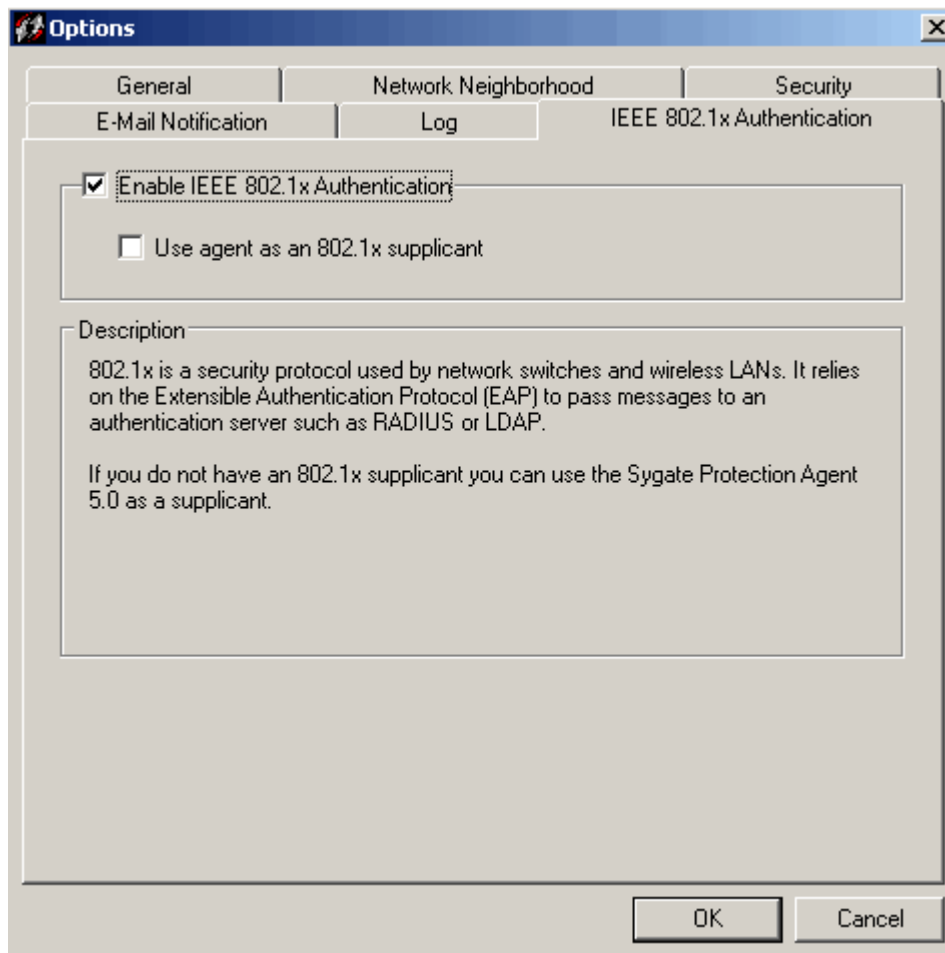


Figure 13. Options: IEEE 802.1x Authentication Tab

Enable IEEE 802.1x Authentication

This option is only available in Client Control mode and only relevant if your installation includes a LAN Enforcer and the system administrator has implemented 802.1x authentication. A LAN Enforcer connects to a switch or wireless access point and can connect to a RADIUS server for additional authentication. Check with your system administrator before setting this option.

Enable Transparent Mode

In LAN Enforcer transparent mode, which uses the Sygate Agent as an 802.1x supplicant, you enable Agents for 802.1x authentication and also enable the Agents as 802.1x supplicants. In transparent mode, you can use either Sygate Protection Agents or Sygate Enforcement Agents.

Setting Up Advanced Rules

Unlike individual application rules, Advanced Rules apply to all applications. If you create an advanced rule that blocks all traffic between 10 PM and 8 AM, the rule will override all other schedules and configurations that have been set for each application.

➡ **Option Alert:** This option is available in Client Control and Power User Mode only.

To set up an advanced rule:

1. On the **Tools** menu, click **Advanced Rules**. The Advanced Rules dialog box opens.
2. Click **Add**. The Advanced Rule Settings dialog box opens with the **General** tab displayed.
3. Enter a name for the rule in the **Rule Description** text box, and click **Block this traffic** or **Allow this traffic**.
4. Click the **Applications** tab, and either click the check box for the application you want to allow or block, or click the **Browse** button to locate it.
5. To create a rule with the default settings, click **OK**. You can also customize settings on any of the tabs: **General**, **Hosts**, **Ports and Protocols**, **Scheduling**, and **Applications**.
6. Click the **Move Up** or **Move Down** buttons to change the order in which the rule is applied.

Note: Rules are applied in the order they are listed. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the Agent blocks all traffic regardless of the other rule.

7. To enable a rule on the Agent, make sure the check mark appears in the **Description** column.

General Tab

The **General** tab is used to provide a name for the rule you are creating, as well as the effect that the rule will have (allowing or blocking traffic).

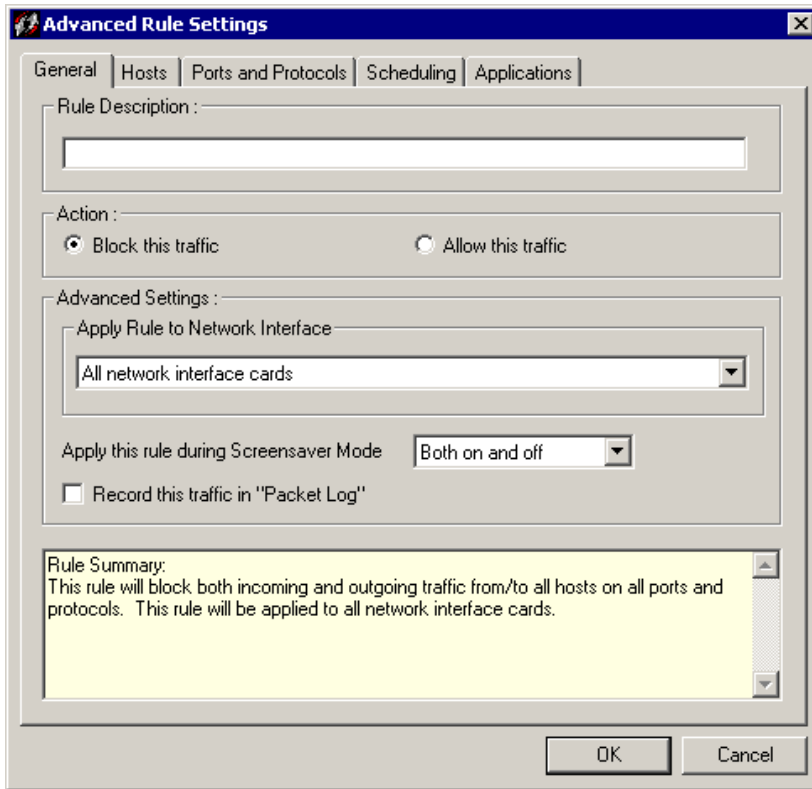


Figure 14. Advanced Rules: General Tab

Rule Description

Functions as the name of the rule, and it should indicate qualities of the rule. For instance, “Rule1” may not be a very good name for a rule, but “Block After 1 AM” would be.

Block this traffic

Denies traffic specified by the rule from accessing your network.

Allow this traffic

Allows this traffic specified by the rule to access your network.

Apply Rule to Network Interface

Specifies which network interface card this rule applies to. If you have multiple network cards, select one from the list box, or select **All network interface cards** to apply the rule to every card.

Apply this rule during Screensaver Mode

Activates the rule even if your computer's screensaver is on (if applicable).

- **On**—The rule is activated only when the screensaver is on. Enable this if you want to block all traffic and all ports while your computer is idle.
- **Off**—This rule is activated only if the screensaver is off and all other conditions are satisfied.
- Both **On** and **Off**—This rule is unaffected by the screensaver.

Record this traffic in "Packet Log"

Records traffic affected by this rule in the Packet Log.

Rule Summary field

Provides a summary of the rule's functionality.

Hosts Tab

From the **Hosts** tab, you can specify the source (IP address, MAC address, or subnet range) of traffic.

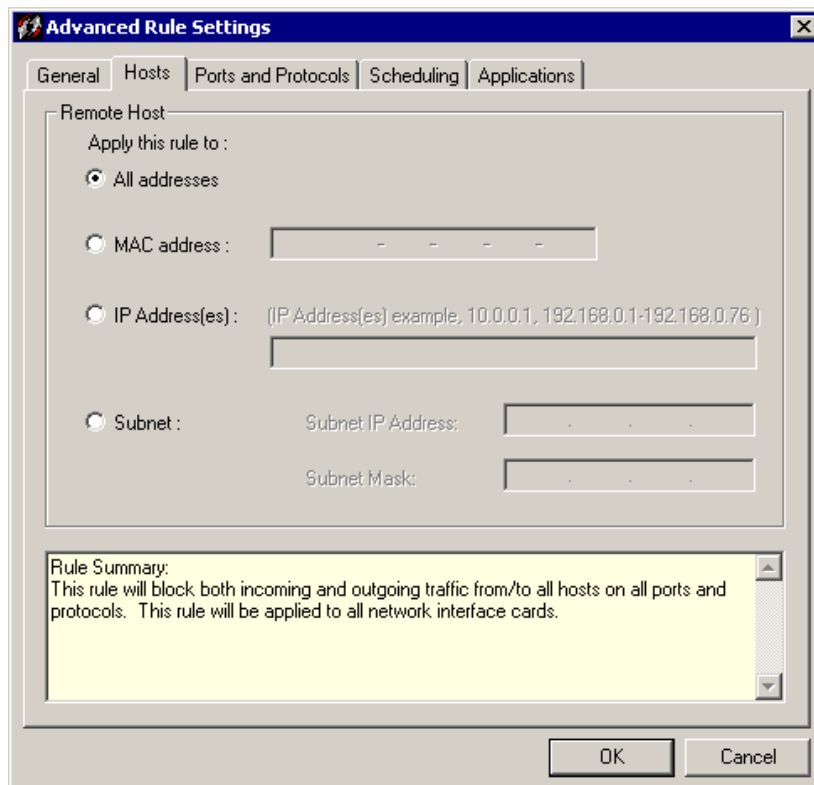


Figure 15. Advanced Rules: Hosts Tab

All addresses

Applies the rule to all addresses.

MAC addresses

Applies the rule to the MAC address of the traffic.

IP Address(es)

Applies the rule to the IP address or address range of the traffic.

Subnet

Applies the rule to the subnet address and subnet mask of the traffic.

Rule Summary field

Provides a summary of the rule's functionality.

Ports and Protocols Tab

The **Ports and Protocols** tab provides an area to specify which ports and protocols, if any, should be affected by the traffic specified in the rule.

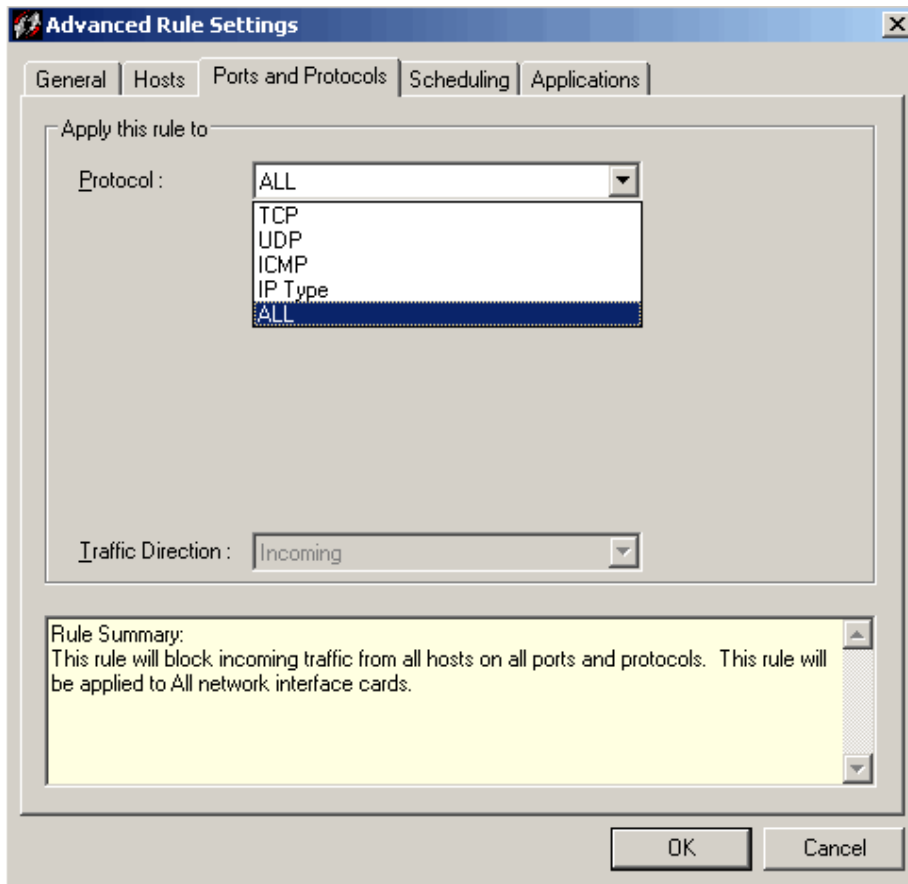


Figure 16. Advanced Rules: Ports and Protocols Tab

Protocol

Specifies a protocol for the rule.

All Protocols

Applies to all protocols on all ports, for both incoming and outgoing traffic.

TCP

Displays two more list boxes in which you can specify which ports (remote and/or local) will be affected by the rule. You can type the port numbers or select the port type from the list boxes for the both local and remote ports.

If you do not enter or select a port number, then all ports are affected by the rule. If you enter a port number for the local port entry, but not for the remote port entry, then the local port you entered and ALL remote ports are affected by the rule.

You can also select which traffic direction should be affected by the rule.

UDP

Displays two port list boxes. You can type the port numbers, or select the port type from the list boxes for both local and remote ports. If you do not enter or select a port number, then all ports will be affected by the rule. If you enter a port number for the local port entry, but not for the remote port entry, then the local port you entered and ALL remote ports will be affected by the rule.

You can also select which traffic direction should be affected by the rule.

ICMP

Displays a list of ICMP types. Select the types of ICMP that you wish allow or block. Then select which traffic direction should be affected by the rule.

IP Type

Displays a list of IP protocol types displayed on the lower half of the **Ports and Protocols** tab.

Traffic Direction

In Advanced rules, there is no traffic direction control.

Rule Summary field

Provides a description of the rule and what traffic it affects on your system.

Scheduling Tab

Using the **Scheduling** tab you can create a rule that only takes effect during (or excluding) certain time periods. For instance, if you want to block all traffic after 1 AM, then you can create a schedule to do so.

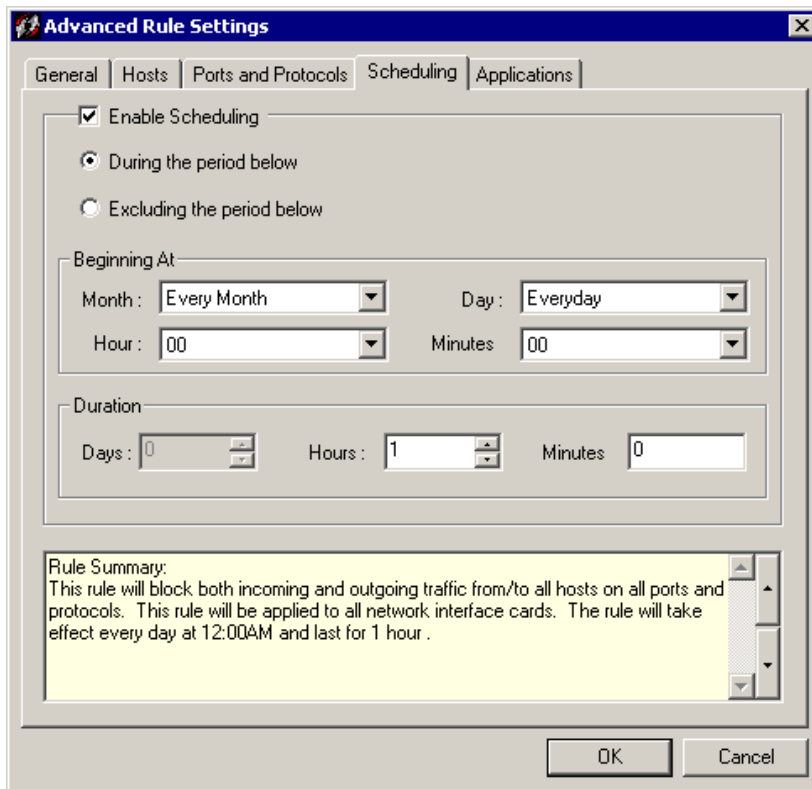


Figure 17. Advanced Rules: Scheduling Tab

Enable Scheduling

Enables the scheduling feature.

During the period below

Enables scheduling to take place during a certain time period.

Excluding the period below

Enables scheduling to take place outside of a certain time period.

Beginning At

Specifies the time that the scheduling begins, including the month, day, hour, and minute. You can also leave the default settings, which apply the schedule all day, every day, all year.

Duration

If you have specified a beginning time, specifies how long the rule will be in effect.

Rule Summary field

Provides a summary of the rule's functionality.

Applications Tab

You can specify the applications affected by the rule. The **Applications** tab provides a list of all applications that have accessed your network connection.

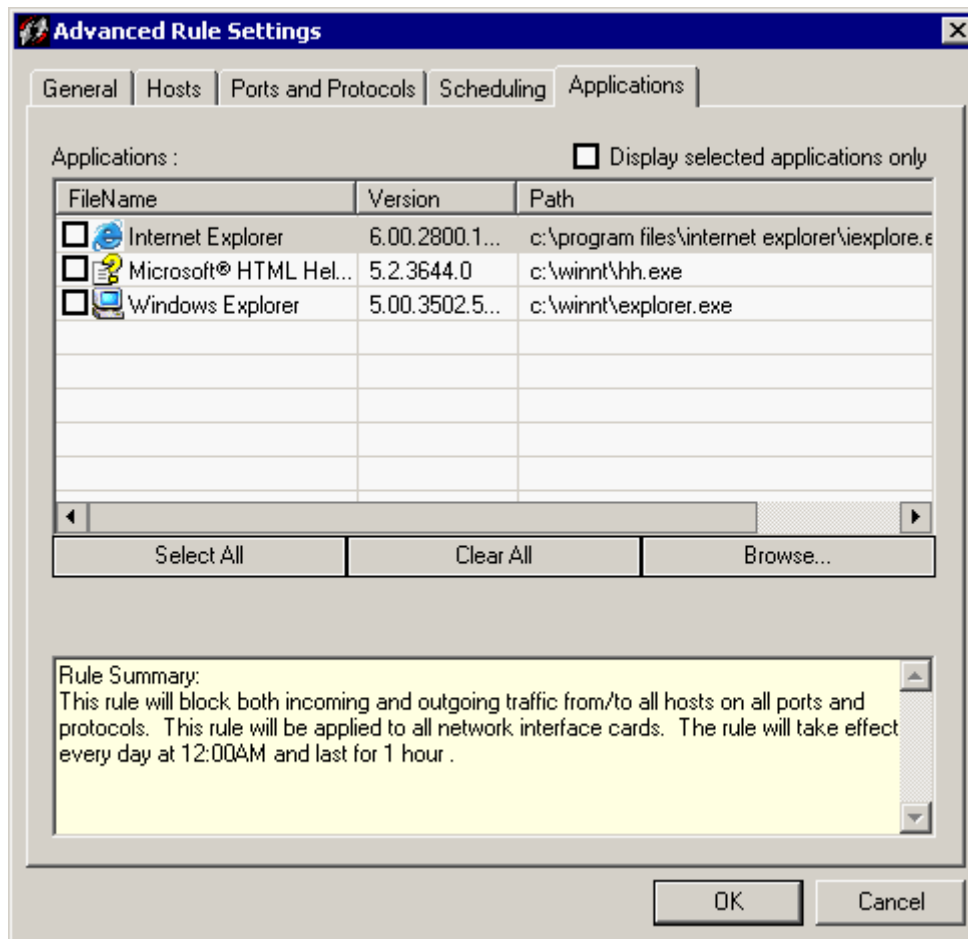


Figure 18. Advanced Rules: Applications Tab

Display selected applications only

Displays only the applications that are controlled by this rule.

Applications

Lists the traffic coming in and out of all ports and protocols. To select an application, click the box next to its name under the **FileName** column.

Select All

Selects all applications in the table.

Clear All

Clears all applications in the table.

Browse

Opens the Open dialog box so you can search for applications that are not displayed in the table.

Rule Summary field

Provides a description of the rule and what traffic it affects on your system.

Viewing Server and Agent Rules

The Security Rule Viewer (the Rule Viewer) displays which *security policies*, or set of security rules, are in effect on your computer.

➡ **Option Alert:** This option is available in the Power User Mode only.

It shows you *server rules*, the rules that the Policy Manager has deployed on your computer, *Agent rules*, and the rules you have created yourself. These are all presented in a single viewer that shows each rule or setting, a description of that rule or setting, and the action that the rule causes (Allow or Block).

To open the Security Rule Viewer:

- On the **Tools** menu, click **Security Rule Viewer**.

The Security Rule Viewer

The Security Rule Viewer provides you with an integrated view of the security rules and settings that are running on your Agent. Agent rules are merged with server rules.

All rules appear in a numbered list in the Rule Viewer. *Server rules* appear first and are listed with a number, the wording “**Server Rule;**” and a brief description of the rule. Clicking a rule displays a summary of the rule in the summary box at the bottom of the screen.

If the rule is an Agent rule, clicking the rule takes you directly to the Applications List, the Configuration Options dialog box, or the Advanced Rule Settings dialog box, where you can fine-tune the rule.

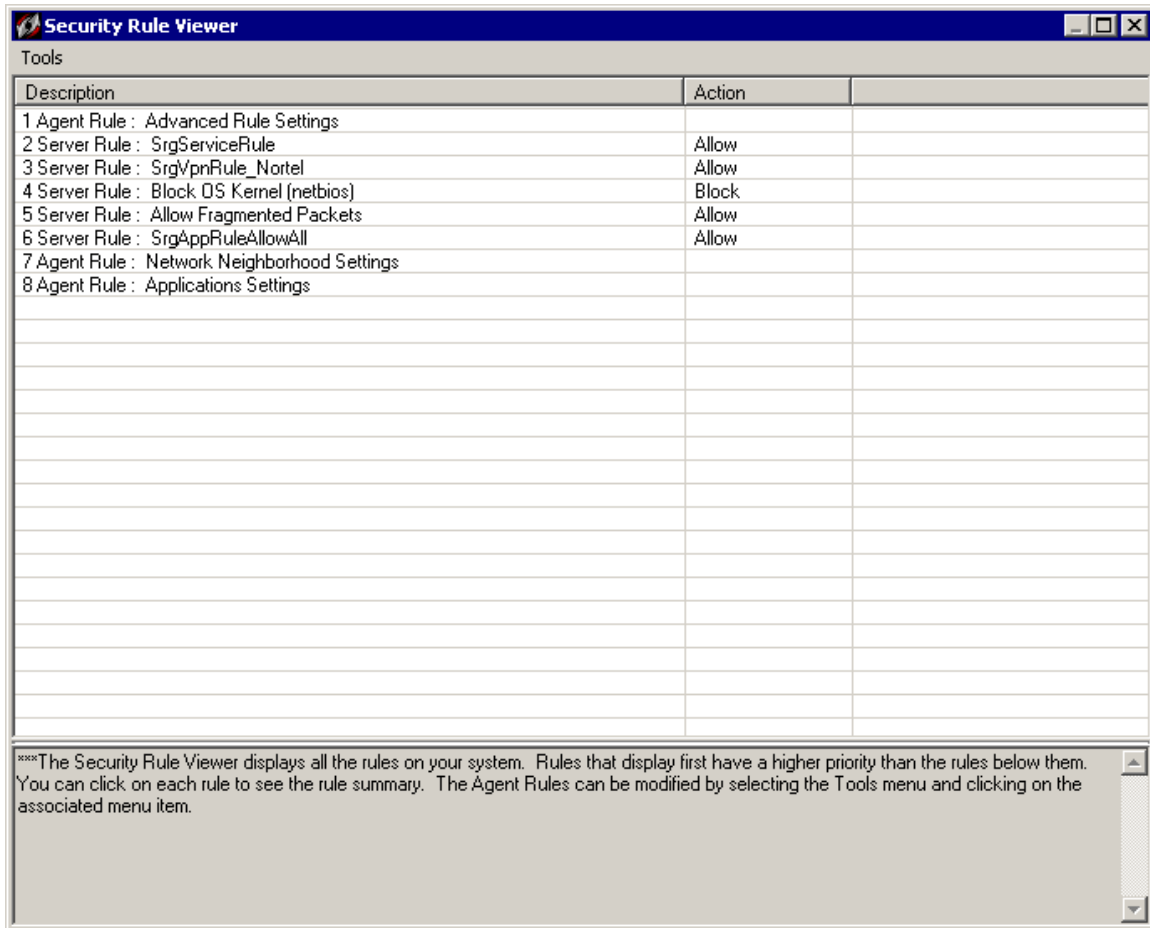


Figure 19. Security Rule Viewer

Order of Priority for Agent Rules versus Server Rules

The order of priority:

1. **Server Rules with high priority levels** as assigned by the system administrator
2. **Agent Advanced Rules**
3. **Server Rules with lower priority levels**
4. **Agent Network Neighborhood** Settings
5. **Agent Application** Settings

Chapter 5. Monitoring and Logging

The Agent's *logs* are an important method for tracking your computer's activity and its interaction with other computers and networks. The logs record information about the Agent's status and about traffic attempting to enter or exit your computer through your network connection.

There are five separate logs that monitor different aspects of your network connection:

- Security log
- Traffic log
- Packet log
- System log
- Behavior log

These logs tell you when your computer has been blocked from the network and to some extent why. They are particularly useful in detecting potentially threatening activity such as port scanning. They also help you troubleshoot connectivity problems or possible network attacks.

All logs are regularly uploaded to the Policy Manager, where they can be used for overall security analysis. These uploads occur at each heartbeat.

You can also use the Agent logs to do back tracing, which enables you to use ICMP to determine all the hops between your computer and an intruder on another computer.

The Agent's *logs* are an important method for tracking your computer's activity and its interaction with other computers and networks. The logs record information about the Agent's status and about traffic attempting to enter or exit your computer through your network connection.

There are five separate logs that monitor different aspects of your network connection:

- Security log
- Traffic log
- Packet log
- System log
- Behavior log

These logs tell you when your computer has been blocked from the network and to some extent why. They are particularly useful in detecting potentially threatening activity such as port scanning. They also help you troubleshoot connectivity problems or possible network attacks.

All logs are regularly uploaded to the Policy Manager, where they can be used for overall security analysis. These uploads occur at each heartbeat.

You can also use the Agent logs to do back tracing, which enables you to use ICMP to determine all the hops between your computer and an intruder on another computer.

Viewing Logs

To view logs on the Agent:

1. Do one of the following:
 - Click **Tools | Logs**.
 - On the toolbar, click the drop-down arrow next to the **Logs** icon.



Note: Click the **Logs** icon to display the most recently viewed log.

2. Click one of the following log types: **Security Log**, **Traffic Log**, **Packet Log**, **System Log**, or **Behavior Log**.

Each log opens the **Log Viewer** dialog box. The Log Viewer is a data sheet, where each row represents a logged event, and the columns display information regarding the event. For more information on the differences between the icons and parameters of each log, see Security Log, Traffic Log, Packet Log, System Log, and Behavior Log.

3. In the Log Viewer dialog box, click the **View** menu and click either **Local View**, the default setting, or **Source View**.

The fields in the log change depending on whether you choose the local view or source view.

4. In the **View** menu, click a different log name if you wish.
5. Click **Refresh** or press **F5** to update the log that you are viewing.
6. Click **File | Exit** to close the log.







Traffic Log

Whenever your computer makes a connection through the network, this transaction is recorded in the Traffic Log.

Icons for the Traffic Log

When you open a Traffic Log, icons are displayed at the left side of the first column. They are graphical representations of the kind of traffic logged on each line and provide an easy way to scan the Traffic Log. Traffic Log includes information about incoming and outgoing traffic.

Table 8. Traffic Log Icons

Icon	Description
	Incoming traffic; passed through the Agent
	Incoming traffic; blocked by the Agent
	Outgoing traffic; passed through the Agent
	Outgoing traffic; blocked by the Agent
	Traffic direction unknown; passed through the Agent
	Traffic direction unknown; blocked by the Agent

Traffic Log Parameters and Description

The columns for logged events are:

Table 9. Traffic Log Parameters and Description

Name of Parameter	Description
Time	The exact date and time that the event was logged
Action	Action taken by the Agent: Blocked, Asked, or Allowed
Severity	The severity of the traffic, set to 10
Direction	Direction that the traffic was traveling (incoming or outgoing)

Table 9. Traffic Log Parameters and Description

Name of Parameter	Description
Protocol	Type of protocol - UDP, TCP, and ICMP
Remote Host	Name of the remote computer <i>(only appears in Local View - this is the default)</i>
Remote MAC	MAC address of the remote device. If outside the subnet, it is the MAC address of the router. <i>(only appears in Local View - this is the default)</i>
Remote Port/ICMP Type	Port and ICMP type on the remote computer <i>(only appears in Local View - this is the default)</i>
Local Host	IP address of the local computer <i>(only appears in Local View - this is the default)</i>
Local MAC	MAC address of the local computer <i>(only appears in Local View - this is the default)</i>
Local Port/ICMP Code	Port and ICMP code used on the Agent computer <i>(only appears in Local View - this is the default)</i>
Application Name	Name of the application associated with the attack
User	Login name of the user
Domain	Domain of the user
Location	The Location (Office, Home, VPN, etc.) that was in effect at the time of the attack
Occurrences	Number of packets each piece of traffic sends between the beginning and ending time
Begin Time	Time traffic starts matching the rule
End Time	Time traffic stops matching the rule
Rule Name	The rule that determined the passing or blockage of this traffic

Description and Data Fields for the Traffic Log

Below the rows of logged events are the **Description** and **Data** fields. When you click an event row, the entire row is highlighted. A description of the event is displayed in the **Description** field.

Packet Log


The Packet Log captures every packet of data that enters or leaves a port on your computer. The Packet Log is disabled by default in the Agent because of its potentially large size. You must enable the Packet Log first.

➡ **Option Alert:** If you do not see the **Options** menu item, the Packet Log is not available on your Agent.

Icons for the Packet Log

There is only one icon displayed in the Packet Log. It indicates the capturing of raw data packets.

Table 10. Packet Log Icons

Icon	Description
	Full data packet captured

Packet Log Parameters and Description

The columns for logged events are:

Table 11. Packet Log Parameters and Description

Name of Parameter	Description
Time	The exact date and time that the packet was logged
Remote Host	Name of the remote computer (<i>only appears in Local View - this is the default</i>)
Remote Port	Port on the remote host that sent/received the traffic (<i>only appears in Local View - this is the default</i>)
Local Host	IP Address of the local computer (<i>only appears in Local View - this is the default</i>)
Local Port	Port used on the Agent computer for this packet (<i>only appears in Local View - this is the default</i>)
Source Host	Name of the source computer (<i>only appears in Source View</i>)
Source Port	Port on the source host that sent/received the traffic (<i>only appears in Source View</i>)
Destination Host	IP Address of the destination computer (<i>only appears in Source View</i>)
Destination Port	Port used on the destination computer for this packet (<i>only appears in Source View</i>)

Table 11. Packet Log Parameters and Description

Name of Parameter	Description
Direction	Direction that the traffic was traveling (incoming or outgoing)
Action	Action taken by the Agent: Blocked or Allowed
Application Name	Name of the application associated with the packet

Packet Decode and Packet Dump for the Packet Log

Below the **Log Viewer** are two additional data fields that provide further detail regarding the selected event. In the Packet Log, these fields are labeled **Packet Decode**, which provides data on the type of packet logged, and **Packet Dump**, which records the actual data packet.




System Log

The System log records all operational changes such as the starting and stopping of services, detection of network applications, software configuration modifications, and software execution errors. It also logs communication with the Policy Manager, including connection and downloads. All information provided in the System Log also appears in real-time in the Message Console. The System Log is especially useful for troubleshooting the Agent.

Icons for the System Log

When you open the System Log, icons are displayed at the left side of the first column. These are graphical representations of the kind of event logged on each line, and they provide an easy way to scan the System Log for possible system errors.

Table 12. System Log Icons

Icon	Description
	Error with the Policy Manager
	Warning; potential problem with the Policy Manager
	Information regarding the Policy Manager

System Log Parameters and Description

The columns for logged events are:

Table 13. System Log Parameters and Description

Name of Parameter	Description
Time	The date and time that the event was logged
Type	The type of event can be an Error, Warning, or Information. An Error log indicates a problem with the source; a Warning log indicates a potential problem; and an Information log provides information about an event involving the Agent.
ID	The ID assigned to the event by the Agent
Summary	Summary description of the event

Description and Data Fields for the System Log

Below the rows of logged events are the **Description** and **Data** fields. When you click on an event row, the entire row is highlighted. A description of the event, such as “Install WsProcessSensor successful....,” appears in the **Description** field.





Security Log

The Security Log records potentially threatening activity directed towards your computer, such as port scanning, or denial of service attacks. The Security Log is probably the most important log file in the Agent.

Icons for the Security Log

When you open a Security Log, icons are displayed at the left side of the first column. These are graphical representations of the kind of attack logged on each line. They provide an easy way to scan the Security Log for possible system errors.

Table 14. Security Log Icons

Icon	Description
	Critical attack
	Major attack
	Minor attack
	Information

Security Log Parameters and Description

The columns for logged events are:

Table 15. Security Log Parameters and Description

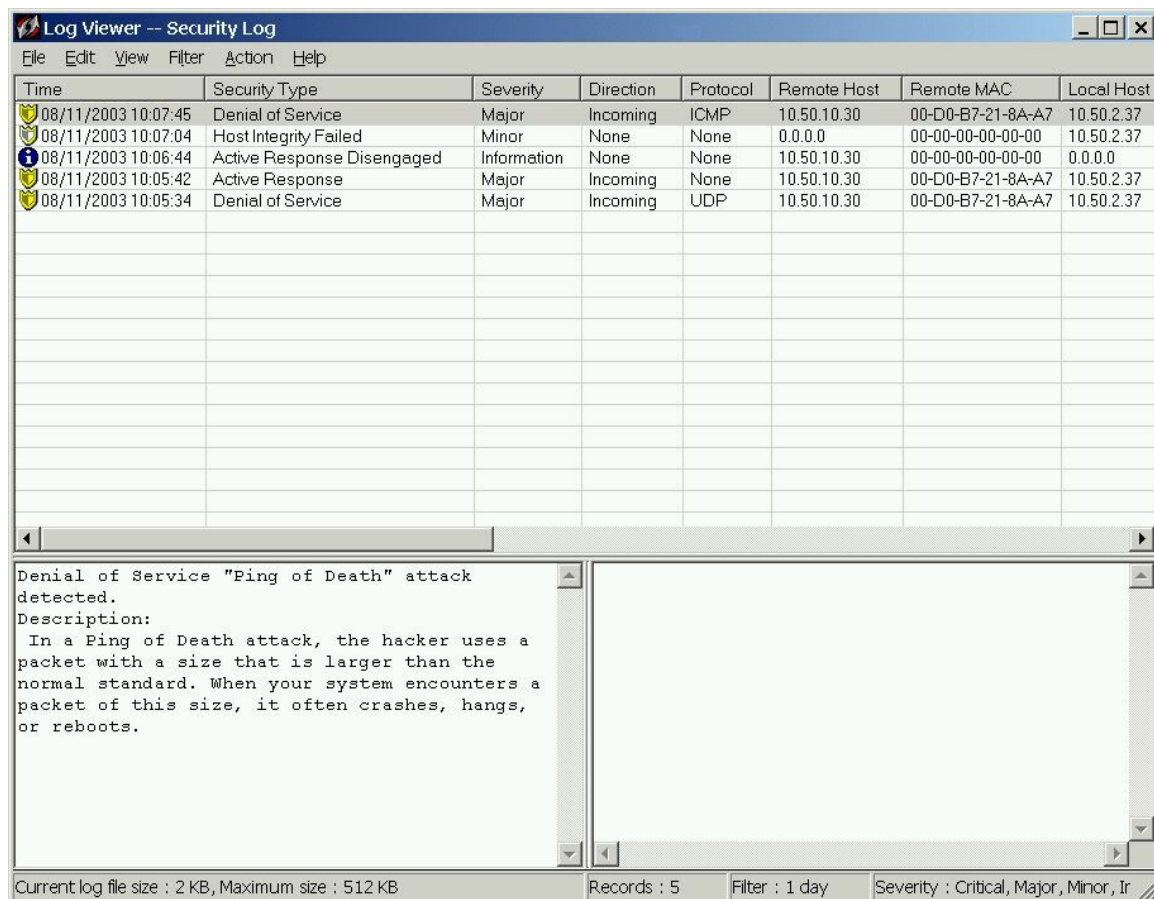
Name of Parameter	Description
Time	The exact date and time that the event was logged
Security Type	Type of Security Alert (for example: DoS attack, executable file, Ping of Death)
Severity	The severity of the attack (either Critical, Major, Minor, or Information)
Direction	Direction that the traffic was traveling (incoming, outgoing, or unknown)—Most attacks are incoming, that is, they originate from another computer. Other attacks, like Trojan horses, are programs that have been downloaded to your computer and therefore are already present. They are considered outgoing. Still other attacks are unknown in direction; they include Active Response or application executable changes.
Protocol	Type of protocol—UDP, TCP, and ICMP
Source Host	Name of the source computer (<i>only appears in Source View</i>)
Source MAC	MAC address of the source computer (<i>only appears in Source View</i>)
Destination Host	IP address of the destination computer (<i>only appears in Source View</i>)
Destination MAC	MAC address of the destination computer (<i>only appears in Source View</i>)
Remote Host	Name of the remote computer (<i>only appears in Local View - this is the default</i>)
Remote MAC	MAC address of the remote device. If outside the subnet, it is the MAC address of the router. (<i>only appears in Local View - this is the default</i>)
Local Host	IP address of the local computer (<i>only appears in Local View - this is the default</i>)
Local MAC	MAC address of the local computer (<i>only appears in Local View - this is the default</i>)
Application Name	Name of the application associated with the attack
User Name	User or Computer client that sent or received the traffic
Domain	Domain of the user

Table 15. Security Log Parameters and Description

Name of Parameter	Description
Location	Location (Office, Home, VPN, etc.) that was in effect at the time of the attack
Occurrences	Number of occurrences of the attack method
Begin Time	Time the attack began
End Time	Time the attack ended

Description and Data Fields for the Security Log

Below the rows of logged events are the **Description** and **Data** fields. When you click an event row, the entire row is highlighted. A description of the event, such as “Somebody is scanning your computer, with 13 attempts,” appears in the **Description** field.

**Figure 20. Log viewer**

Behavior Log

Your administrator has probably set up some OS Protection rules on the Policy Manager. OS Protection policies are security rules and settings that protect the registry, safeguard specific files or directories, control process, DLL, and application execution.

The Behavior Log records the activities specific to an application's behavior. It records the registry keys, files, and DLLs that an application accesses as well as the applications that it runs. If an application performs an activity outside of its allowed range, it is blocked. A web server, for example, serves web pages. It should not be copying files to your system folder. All information provided in the Behavior Log is logged as a result of the OS Protection rules.

The table below explains these fields.

Table 16. Agent Behavior Log Parameters and Description

Name of Parameter	Description
Severity	Severity of the behavior. The options are Severe, Critical, Minor, Information
Action	Action taken by the Agent: Blocked or Allowed, Ignore (the rule triggered but is a pure logging rule), Terminate (process terminated)
Mode	Normal or Test
Description	Description of the behavior on the Agent
VAPI Class Name	Name of the API that caused the logging of this behavior
Time	Exact date and time that the event was logged
Rule Name	Name of the rule that caused the logging of this behavior
Caller Process ID	ID of the process that triggers the logging
Caller Process Name	The name of the process that sent the error
Parameter	Parameters that were used in the API call, converted to STRING and separated by a space character
Location Name	Name of the location the where the application logged in
User Name	Name of the Agent machine or user

Table 16. Agent Behavior Log Parameters and Description

Name of Parameter	Description
Domain Name	Name of the Policy Manager Domain in which the Agent is located

Enabling and Clearing Logs

➡ **Option Alert:** This option is available in the Client Control and Power User Mode only.

The Security, Traffic, Behavior, and System Logs are enabled by default. You must enable the Packet Log before you can view the contents.

To enable the log and set the log size:

1. On the **Tools** menu, click **Options**.
2. Click the **Log** tab.
3. Click the appropriate log check box to enable it.
4. Click the appropriate **Maximum Log File Size is** field and enter a size, in kilobytes, for the log file. 256 KB is the default setting.
5. Click **OK**.

To set the number of days to save the log:

1. On the **Tools** menu, click **Options**.
2. Click the **Log** tab.
3. Click the appropriate log check box to enable it.
4. Click **Save log file for the past** field for the log you want to configure.
5. Enter the number of days.
6. Click **OK**.

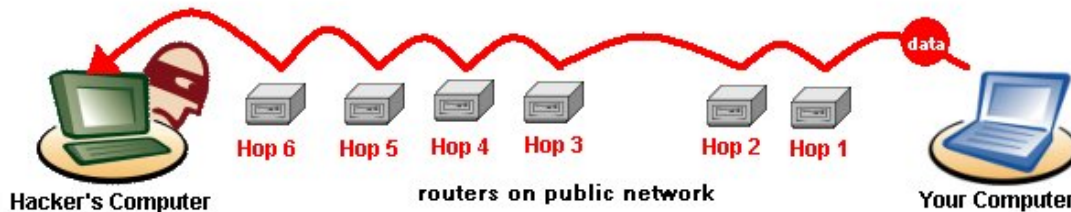
To clear the log:

1. In each log, click **File | Options**.
2. Make sure the Log tab is selected.
3. Click the **Clear Logs** button for the log you want to clear.

Note: For each log, you can also click **File | Clear**.

Back Tracing Logged Events

Back tracing enables you to pinpoint the source of data from a logged event. Like retracing a criminal's path at a crime scene, back tracing shows the exact steps that incoming traffic has made before reaching your computer.



Back tracing is the process of following a data packet backwards, discovering which routers the data took to reach your computer. In the case of a Security Log entry, you can trace a data packet used in an attack attempt. Each router that a data packet passes through has an IP address, which is provided in the **Trace Route** field.

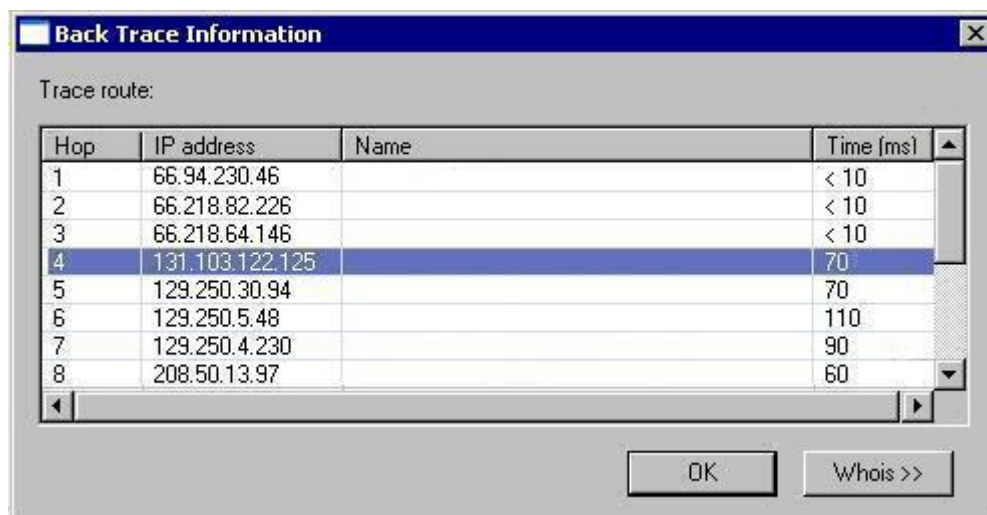
You can back trace a logged event in the Security, Traffic, and System logs.

To back trace a logged event:

1. Open the log file and click an event so that the entire row is selected.
2. Either right-click and click **BackTrace**, or click **Action | BackTrace**.

The Agent begins back tracing the event.

3. The **Back Trace Information** dialog box appears.



The **Trace route** field provides details, such as IP address, on each *hop* made by the data packet that was logged by the Agent. A hop is a transition point, usually a router, that a packet of information travels through as it makes its way from one computer to another on a public network, such as the Internet.

4. To view detailed information on each hop, click the **WhoIs>>** button.

A drop panel displays detailed information about the owner of the IP address from which the traffic event originated. Note that the information displayed does not guarantee that you have discovered who the hacker actually is. The final hop's IP address lists the owner of the router that the hackers connected through, and not necessarily the hackers themselves.

5. Click either **Whois<<** again to hide the information.

Note: You can cut and paste the information in the **Detail information** panel by pressing **Ctrl+C** to copy the information into the Clipboard, and then pasting it (**Ctrl+V**) into an e-mail message to your system administrator.

It is not advisable to contact persons listed in the **Detail information** panel unless you are experiencing a high number of security logs in which the attacks originate from one particular IP address.

6. Click **OK** to return to the **Log Viewer** dialog box.

Filtering Logged Events

After you have opened a log in the **Log Viewer** dialog box, you can view the recorded events in the Log Viewer by the severity level of the attack and by a previous period of time.

To filter log events by severity:

1. In the **Log Viewer** dialog box, click the **Filter** menu.
2. Click **Severity**. The **Severity** submenu appears.
3. Click the severity level(s) so that a check mark appears to the left of the severity level name. You have the following options:
 - **Critical** (*Security Log only*)
 - Major
 - Minor
 - Error (*System Log only*)
 - Warning (*System Log only*)
 - Information

You can view more than one type of event at once. The **Log Viewer** is automatically reloaded.

To filter log events by time period:

1. In the **Log Viewer** dialog box, click the **Filter** menu.
2. Select the time period for which you want to view log events. For example, **2 Week Logs** displays the events recorded over the past 14 days.

The log automatically displays the requested events.

Saving Logs

The contents of the logs can be saved to different locations. You may want to do this to save space. However, it more likely that you do this to send the logs to your system administrator for security review, or to import them into a tool such as Microsoft Excel.

To save a log file:

1. Open the log in the Log Viewer.
2. Click **File | Export**.
3. In the **Save As** dialog box, select the location for the log file.
4. Click **OK**.

Stopping an Active Response

Any security attack that is detected on the Agent triggers an active response. The active response automatically blocks the IP address of a known intruder for a specific amount of time (the default is 10 minutes). If you don't want to wait the default amount of time to unblock the IP address, you can stop the active response immediately. Your system administrator sets the default amount of time in the Policy Manager.

You can stop active responses in the Security Log only.

To stop an active response:

1. On the main console, click **Tools | Logs | Security**.
2. Select the row for the application or service you want to unblock. Blocked traffic is specified as **Blocked** in the **Action** column.
3. On the **Action** menu, click **Stop Active Response** to block the selected application, or click **Stop All Active Response** if you want to unblock all blocked traffic.
4. When the **Active Response** dialog box appears, click **OK**.

Responding to Access Status Pop-up Messages

➡ **Option Alert:** This option may not be available in your control mode.

If you or your system administrator has set your applications' permission status to **Ask** or **Block**, an application pop-up message appears when an incoming application is accessing your computer. You can respond to the pop-up message as follows.

Table 17. Agent Application Access Status

If you click	If you check "Remember my answer..." box?	Your Agent will...
Yes	Yes	Allow the application and don't ask again.
Yes	No	Allow the application and ask you every time.
No	Yes	Block the application and ask you every time.
No	No	Block the application and don't ask you again.

To change the access status of an application, you can change its status from the Applications List.

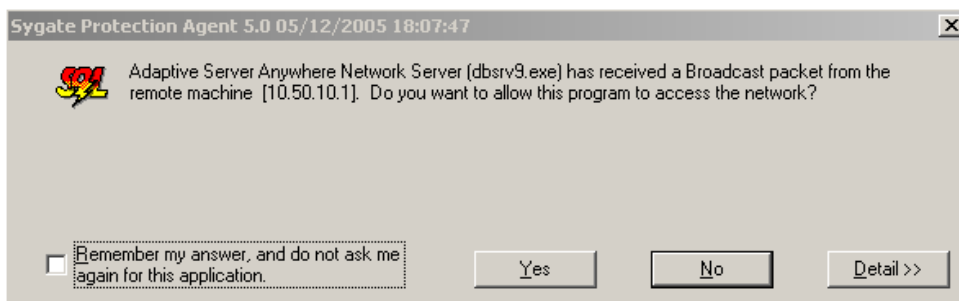
Chapter 6. Messages and Warnings

You may see several different types of messages. These messages will usually describe the situation and indicate how the Policy Manager is attempting to resolve the issue.

The two main types of pop-up messages are:

- security notifications
- warning messages

These are examples of Security warnings.



Here is an example of a Warning message:



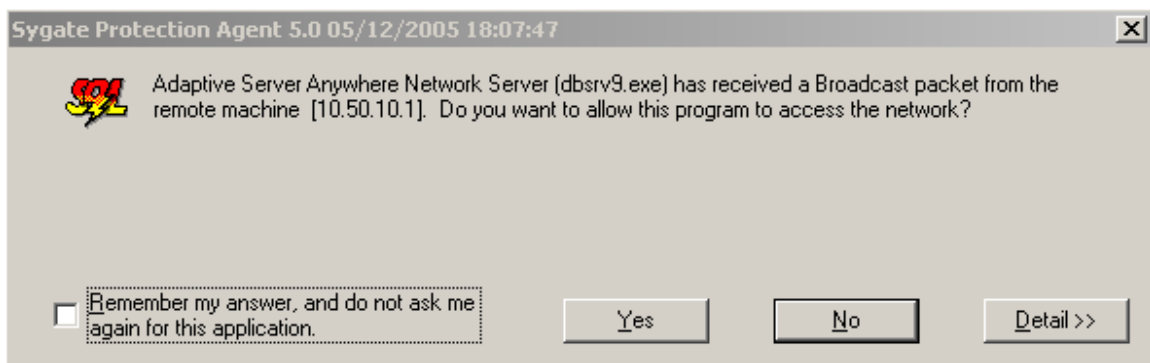
Why Did I Get a Pop-up Message?

An application-related pop-up message occurs for one of the following reasons:

- An application that the Agent has never seen before, or that has been assigned the status of “Ask” is trying to access your network connection.
- An application that normally accesses your network connection has changed, possibly because of a product upgrade.
- You are using Windows XP, and have switched users using Fast User Switching.
- Your Agent software is being updated.
- The Agent has detected a Trojan horse on your Computer.

New Application Pop-up

You may occasionally see the following pop-up message on your computer screen.



What Does This Mean?

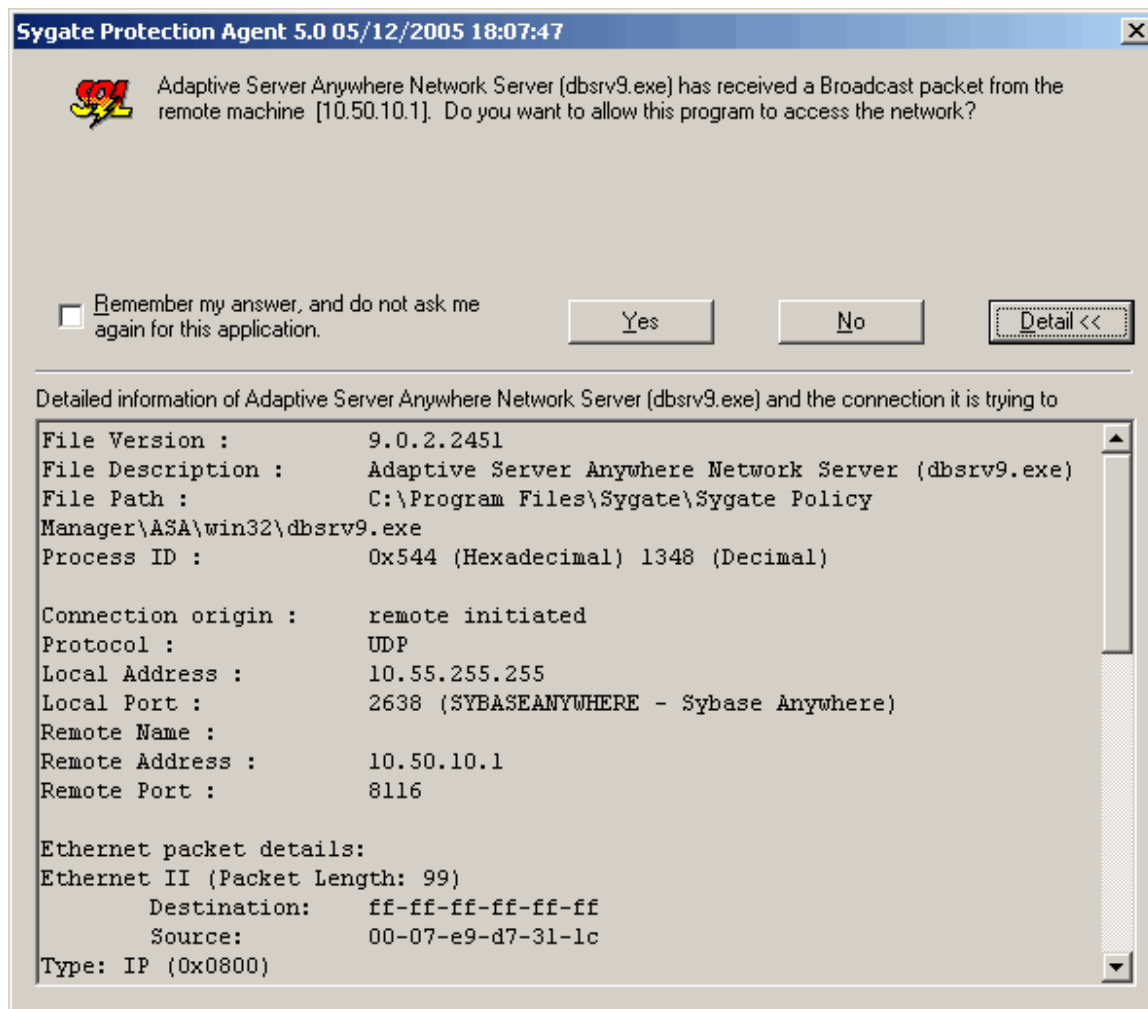
The information in the pop-up tells you what application or service is trying to access your computer, what port and often other information.

This pop-up appeared because the application has been opened, either directly by you, indirectly by you, or by another application.

What if you didn't open any program or click any link, and a program suddenly tries to access your network connection? Again, there could be a number of different reasons. However, if you haven't opened any programs that use the application listed on the pop-up message, or can't see any reason why that application should try to access your network connection, it is always safest to click No. This might indicate the presence of a Trojan horse on your computer, something that needs to be checked immediately.

Detail

Clicking the Detail button expands the pop-up box, providing further details on the connection the application is attempting to establish. Information such as the file name, version, and path are provided. Look at these items to make sure that they match the description of the application that you normally use. The details section should also indicate the location to which the file was attempting to connect: either local (meaning that it was trying to connect to your computer, or remote (meaning that the application was attempting to connect to an outside destination). Additionally, the local and remote port numbers and IP addresses should be provided, as shown in the following illustration:



What Should I Do?

This kind of message is common when you first start using the Agent. If you believe that you have triggered this application, it would be safe to click Yes. You have the option to tell the Agent to remember your answer in the future. If you click Remember my answer, and do not ask me again for this application, the Agent will remember your choice, and will act accordingly the next time this application tries to access your network connection.

If you have tried to open an application (such as a web browser) or a program that uses another application to access the Internet (such as a media streaming program) and you feel comfortable granting this application access to your network connection, then you can click Yes. The application will then be able to access your network. You can change the status of the application at any time, either in the Running Applications field or in the Applications List.

However, if a pop-up message is unexpected, and you can't see any reason why the listed application should try to access your network connection, click No, and click Remember my answer. This will assign the application the status of Block, so that it will be automatically blocked from your network connection any time it tries to gain access. You can change the status of the application at any time, either in the Running Applications field or in the Applications List.

You should also run a virus scan to make sure that you have not inadvertently downloaded a virus or a Trojan horse that could infect your computer files.

Table 18. Pop-up: Remember My Answer?

Click	Check "Remember my answer..." box?	Status Assigned
Yes	Yes	Allow
Yes	No	Ask
No	Yes	Block
No	No	Ask

Changing the Status of an Application

What if you change your mind about an application after you have allowed it or blocked it? Simply go to the main console of the Agent, right-click the application's icon in the Running Applications field, and click the desired status (**Allow**, **Ask**, or **Block**) from the menu that appears.

Changed Application Pop-up Messages

Occasionally, you might see a pop-up message that indicates an application has changed.

"Telenet Program has changed since the last time you opened it, this could be because you have updated it recently. so you want to allow it to access the network?"

What Does This Mean?

The application listed on the pop-up message is trying to access your network connection. Although the Agent recognizes the name of the application, something about the application has changed since the last time the Agent encountered it.

This could be because you have upgraded the product recently. The Agent uses an MD5 checksum to determine the legitimacy of an application. An upgraded version might not pass the checksum test, since a new build or new version of the application is likely to have a different checksum value.

On the other hand, if you have not recently upgraded the application, and see no reason why this message should appear, this could be an instance of a Trojan horse trying to access your network.

Detail

Clicking the Detail button expands the pop-up box, providing further details on the connection the application is attempting to establish. Information such as the file name, version, and path are provided. Look at these items to make sure that they match the description of the application that you normally use. The details section should also indicate the location to which the file was attempting to connect: either local (meaning that it was trying to connect to your computer, or remote (meaning that the application was attempting to connect to an outside destination). Additionally, the local and remote port numbers and IP addresses should be provided.

What Should I Do?

If you have recently upgraded the application mentioned on the pop-up message, it is probably safe to click Yes and allow the application network access. However, if you do not think that you have recently upgraded the listed application, you should click No and run an antivirus software program. If you are at work, contact your IT department.

Changing the Status of an Application

What if you change your mind after allowing or blocking an application? Simply go to the main console of the Agent, right-click the application's icon in the Running Applications field, and click the desired status (Allow, Ask, or Block) from the menu that appears.

Fast User Switch Pop-up Message

If you are using Windows XP, you may see one of the following pop-up messages:

"Sygate Protection Agent is unable to show the user interface. If you are using Windows XP Fast User Switching, make sure all other users are logged off of Windows and try logging off of Windows and then log back on. If you are using Terminal Services, the user interface is not supported."

or

"Sygate Protection Agent was not running but will be started. However, the Sygate Protection Agent is unable to show the user interface. If you are using Windows XP Fast User Switching, make sure all other users are logged off of Windows and try logging off of Windows and then log back on. If you are using Terminal Services, the user interface is not supported."

What Does This Mean?

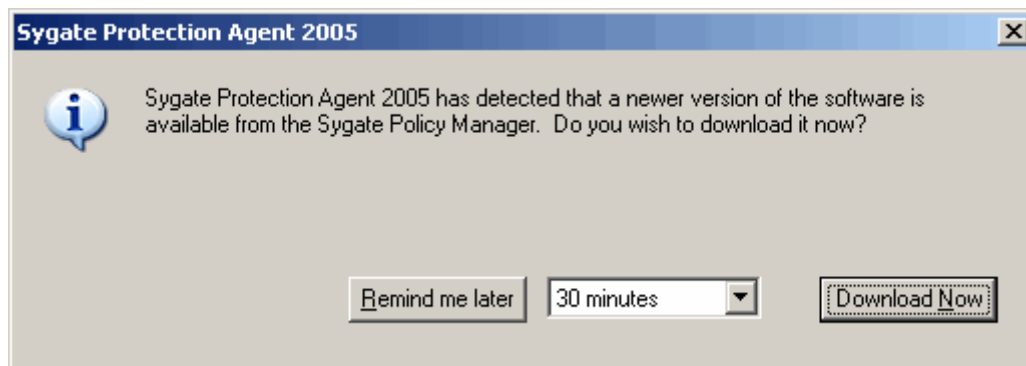
Fast User Switching, a feature of Windows XP Home Edition and Windows XP Professional when it is not joined to a domain, makes it possible for you to quickly switch between users without actually logging off from the computer. Multiple users can share a computer and use it simultaneously, switching back and forth without closing the programs they are running. One of these windows appears if you switch users using Fast User Switching.

What Should I Do?

Follow the instructions in the dialog box.

Automatic Update Notification

Your Agent can be automatically updated by the Management Server. You may see one of the following notification pop-up messages:



If you see this dialog box, you can either download the software immediately, or ask to be reminded later. When that time comes, you have the same choice. This message also appears if you do not have the "Remind me later" option. In that case, you may be simply notified that an upgrade is taking place.

Once the download completes and the software is upgraded, you see the following message:



Trojan Horse Warning

Hopefully, you will never see a pop-up message like the following:

"C:\WINNT\System32\UMGR32.EXE, a Trojan horse application has been detected on your computer. It has been blocked by the Sygate Protection Agent."

What Does This Mean?

This message indicates that the Agent has detected a known Trojan horse on your computer. It also explains that the Trojan horse has been blocked from accessing your network.

This means that a Trojan horse is present on your system and has been activated. Either you tried to open the program identified as a Trojan horse, or it has been triggered by another program on your computer. It is possible that the Trojan was on your computer when you installed the Agent, or that you have recently downloaded it through a legitimate application, such as a web browser. The Trojan tried to access your network connection, and has been blocked by the Agent.

What Should I Do?

You should immediately notify your IT department. The Agent will block the Trojan from sending any information out of or into your computer, but it is still important to remove it from your system as soon as possible. The Agent will terminate the Trojan process automatically, but removal will require the assistance of your IT department.

Why Did I get a Security Notification?

Security notifications are designed to let you know the status of your security. You will see a security notification for one of two reasons:

- **Blocked Application Notification:** An application that has been launched from your machine has been blocked in accordance with rules set by your system administrator. The notification has also been set up by your administrator to inform you of this policy.
- **Security Alert Notification:** There has been an attack launched against your machine, and this notification will either simply inform you of the situation or provide instructions on how to deal with it.

Blocked Application Notification

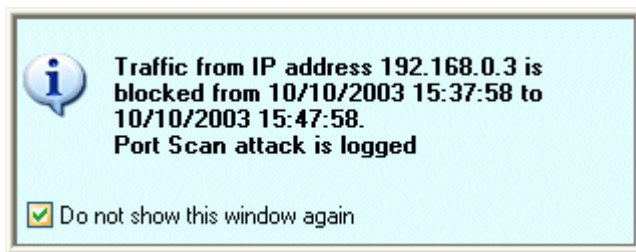
You may see notification messages above your system tray icon from time to time. They indicate that your system has blocked traffic that you have specified as not trusted. Please note that if you are operating under Block All mode, you will see these messages quite often. On the other hand, if you are operating in Allow All mode, you won't see any notifications at all.



If these notifications start annoying you, you can either click **Do not show this window again**, or you can disable these messages altogether in the Options window, under the General Tab.

Security Alert Notification

You may see notification messages above your system tray icon from time to time. The notification pictured below indicates that the Agent has logged an attack.



If you do not want to see these notifications, you can either click Do not show this window again, or you can disable these messages altogether in the Options dialog box, under the General tab.

Why Did I Get a Warning Message?

Warning messages inform you about a problem with your machine that must be corrected before you can access the network. They are based on the host integrity capability that is built into your Agent, the Management Server, and the Enforcer.

You will see messages that indicate that you are lacking the applications needed to connect to the network.

The types of problems that cause warnings include:

- An application is not running that should be running. You are prompted to start it, or your Agent starts it for you.
- An antivirus signature file on your system is out of date. Your Agent goes onto the network to retrieve the file and installs it.
- Your operating system files do not have a required patch. Your Agent goes onto the network to retrieve the patch and installs it.

Your Agent Does An Automatic Download

If your files are not up to date or are missing, your Agent will attempt to connect to the network to download files that solve that problem.

During the download process, you see a progress bar, providing you with information on the process.

Upon conclusion of the process, your Agent will tell you that it has been restored to comply with the latest security policy.

You May Be Blocked From the Network

If your Agent is not running the appropriate software, such as antivirus software, and that software cannot be installed on your computer, your system administrator may have decided to protect the network by blocking your computer from access to the network. Contact your administrator if your Agent gets blocked and can't download the appropriate software.

Glossary

#

802.1x authentication: A standard for passing EAP over a wired or wireless LAN. When the Sygate Enforcer is run as a LAN Enforcer, it performs 802.1x authentication. See LAN Enforcer.

A

access point: A network connection that allows a computer or user to connect to an enterprise network. Virtual Private Networks (VPNs), wireless communications, and Remote Access Service (RAS) dial-up connections are examples of access points. See also end point, wireless access point (wireless AP).

Active Directory: A Microsoft Windows directory service that maintains information about objects connected a network on a server called the Microsoft Windows Active Directory server. Active Directory makes it so network users can log on once to use resources (for which they have been granted access) anywhere on the network. A Policy Manager can import the users from an Active Directory server. See also directory server, LDAP.

Active Response: The ability to automatically block the IP address of a known intruder for a specific amount of time. The amount of time that a Protection Agent blocks an intruder's IP address can be modified to any interval from 1 to 65,000 seconds.

adapter: See network adapter.

Agent: A computer running Sygate Protection Agent or Sygate Enforcement Agent software is also called an Agent computer. Protection Agents can be client controlled or server controlled and can be protected by a firewall, OS Protection, and Host Integrity policies. Enforcement Agents are protected by Host Integrity policies. See also client, Client Control, Server Control, Sygate Protection Agent, Sygate Enforcement Agent.

Anti-IP Spoofing: Sygate Enterprise Protection only. An advanced firewall policy setting that prevents an intruder from taking advantage of the ability to forge (or spoof) an individual's IP address. See also IP Spoofing.

Anti-MAC Spoofing: Sygate Enterprise Protection only. An Intrusion Prevention setting that prevents an intruder from taking advantage of the ability to forge (or spoof) a Media Access Control (MAC) address of a computer. Anti-MAC Spoofing allows incoming and outgoing ARP (Address Resolution Protocol) traffic only if an ARP request has been made to a specific host. It blocks all other unexpected ARP traffic and logs it in a Security Log. See also Smart ARP, MAC address, MAC Spoofing.

antivirus: Software and technology that is used to detect malicious computer applications, prevent them from infecting a system, and clean files or applications that are infected with computer viruses. Sygate software works together with antivirus software. An Enforcer can check whether an Agent is running antivirus software, whether it is the correct version, and whether the current virus definitions (.dat files) are up-to-date. If the program or the .dat files are not current, an Enforcer can install the program, update the .dat files, and start it up. See also virus.

Application Compatibility Pack: A proprietary Sygate .acp file that improves application interoperability with the buffer overrun protection feature. Contact Sygate to discuss Application Compatibility Pack needs.

application control: Applications and what versions of the particular application can either be allowed or disallowed via security policies.

Application Learning: An option that helps system administrators track an Agent's network access and use of applications. If Application Learning is enabled for a specific location, Agents automatically send information about applications that an Agent runs to a Policy Manager. A specific version of that application can then be used for creating a rule. See also Learned Applications.

authentication: The process by which a system identifies an individual or a computer to make sure that the user or computer is who they claim to be. An Enforcer checks whether a client is allowed by reviewing a list of trusted client IP ranges. If the client is not within an acceptable range, the Enforcer sends an authentication packet to the Agent. See also Authentication port.

Authentication port: The port that an Enforcer uses to contact an Agent for authentication. The default UDP port is port 39,999.

authorization: The process of granting or denying access to a specific network resource or domain based on the user's identity.

AutoLocation: The ability to automatically switch to a different location without user intervention. The use of security policies can determine the location and network environment of a user connecting to the corporate network such as when working on-site, working at home, or connecting from another business location. See also AutoLocation ruleset, AutoLocation Switching, location.

AutoLocation ruleset: A set of rules that determine whether or not the location meets the system criteria. Items listed in one AutoLocation ruleset have a conditional OR relationship (one has to be true). Those included in more than one AutoLocation ruleset have an AND relationship (both have to be true). One AutoLocation setting from each AutoLocation ruleset must match before it switches to that location. The AutoLocation ruleset always defaults to the last set used.

AutoLocation Switching: A security policy that allows an Agent to automatically adapt the rules and policies based on the location and network environment. For example, locations named Office, Telecommuter, and Home enforce different security policies depending on where the user logs in. If a client connects to the enterprise network using a Sygate Agent with AutoLocation Switching enabled, the Agent automatically determines which location and therefore which security policy must be enforced based on the client's current network characteristics.

B

backtrace: A way of using ICMP to determine all the hops between your computer and an intruder on another computer. See also Internet Control Message Protocol (ICMP).

broadcast: Sending a packet to everybody on the network. See also multicast, unicast.

buffer overflow: Applications set aside areas of memory, or buffers, for use as storage, frequently setting aside a finite amount of memory for a buffer. A buffer overflow exists when an application attempts to store more data than can fit in a fixed-size buffer. Buffer overflow attacks occur when an intruder is able to send data in excess of a fixed-size application buffer and the application does not check to ensure this doesn't happen. By overflowing a buffer with executable code, an intruder can cause an application to perform unexpected and often malicious actions using the same privileges the application has been granted.

C

client: A computer or program that uses shared resources from another computer, called a server. In the context of Sygate's software, client refers to a Sygate Protection Agent or Sygate Enforcement Agent running on a workstation, desktop computer, or laptop that reports to a Policy Manager. Clients can be organized into groups. See also client group, server, Sygate Protection Agent, Sygate Enforcement Agent, Sygate Policy Manager.

Client Control: A Policy Manager option for setting up a Sygate Protection Agent on a computer so that a user can customize the settings for personal security. This option provides more user control than the Server Control option. See also Server Control, Power User Mode.

client group: Clients that log on to the network are organized into groups. A Policy Manager has two kinds of groups: users and computers. See also Computer group, Users group, Global group.

Communication Channel Encryption: A security feature that allows a Policy Manager administrators to protect or “encrypt” the communication between a web console and a Policy Manager. See also encryption.

computers: A personal computer, laptop, or workstation on which users perform work. In an enterprise environment, computers are connected together over a network. Within Sygate software, a computer refers to an Agent that is a member of a computer-based group. See also Computer group, Sygate Protection Agent.

Console Access Policy: Specifies all IP addresses that are allowed to access a Policy Manager and the computer on which it is installed.

Console Control: Disconnecting the Sygate Enforcer from the Policy Manager so that options can be set on the Enforcer itself, rather than on the Policy Manager. Many of the changes made on the Enforcer will be overwritten when the Enforcer reconnects to the Policy Manager.

custom library: A library containing custom IPS signatures that are created and stored on the Sygate Policy Manager. A custom library can be used in addition to the System Library provided by Sygate. System administrators can add new IPS signatures and signatures from third-party IPS vendors responding quickly to new attacks. A custom library is shown using a yellow icon in the interface. See also signature library, System Library.

D

Data Encryption Standard (DES): An algorithm for protecting data using private encryption keys. DES-CBC is the Cipher Block Chaining (CBC) mode of DES, a stronger form of encryption, which applies an exclusive OR to each block of data with the previous block and then encrypts the data using the DES encryption key. 3DES or Triple DES is the strongest form of encryption where each data block is encrypted three times with different keys. See also encryption.

database replication: The process of distributing changes made from one Sygate Policy Manager to another and then synchronizing the databases for redundancy.

debug log: A text file on the Sygate Policy Manager that includes troubleshooting information such as date and time stamp, current build number, operating system version, errors and events that occur on the Sygate Policy Manager, and also installation and upgrade messages.

Default Location: A setting on the Sygate Policy Manager that specifies the location the Sygate Agent will use when it first starts or if some conflict occurs between two locations during AutoLocation Switching. Default Locations are not inherited. See also AutoLocation Switching, Location.

demilitarized zone (DMZ): A security measure used by a company that can host Internet services and has devices accessible to the Internet; the DMZ is an area between the Internet and the internal network that prevents unauthorized access to the internal corporate network using a firewall or gateway. The Sygate Enforcer can operate in a DMZ providing limited network access so that Agents can connect to a server to update their systems if necessary.

Denial of Service (DoS): A network-based attack that is characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service. See also Denial of Service Checking.

Denial of Service Checking: A Intrusion Prevention setting on the Policy Manager that instructs the Agent to check for incoming traffic using known Denial of Service (DoS) techniques.

DES: See Data Encryption Standard (DES).

destination IP address: The IP address of the computer that is receiving packets of information.

destination port: The port of the computer that is receiving packets of information.

DHCP: See Dynamic Host Configuration Protocol (DHCP).

DHCP Enforcer: Used for enforcement for internal clients that gain access to the LAN by receiving a dynamic IP address through a Dynamic Host Configuration Protocol (DHCP) server. Clients that are running the Sygate Agent and comply with Host Integrity requirements are allowed to connect with the normal DHCP server; otherwise, clients are connected to a quarantine DHCP server.

directory server: Software that manages users' accounts and network permissions. Active Directory is an example of a directory server accessed using Lightweight Directory Access Protocol (LDAP). See also Active Directory, Lightweight Directory Access Protocol (LDAP).

DLL: Dynamic link library, a list of functions or data used by Windows applications. Most DLLs have a file extension of .dll, .ocx, .exe, .drv, or .fon.

DLL authentication: The ability to validate shared or application-specific dynamic link libraries (DLLs) and ensure the integrity of applications. A Sygate Protection Agent can be instructed to allow or block known DLLs. See also file fingerprint, DLL.

domain: A set of clients that are administered by a domain administrator who has a limited view of the Sygate management console (no Servers tab and clients in the domain). Each domain can represent a division, department, separate company, or other isolated segment of users. See also domain administrator.

domain administrator: A person responsible for administering a specific domain including monitoring its security configuration, adding groups and users, and updating Agent software and policies. See also domain.

domain name: The name by which a group of computers is known to the network. Most organizations have a unique name on the Internet that allows individuals, groups, and other organizations to communicate with them. See also domain.

DoS attack: See Denial of Service (DoS).

driver-level protection: A Sygate software feature that blocks protocol drivers from gaining access to the network unless a user gives permission. If a protocol driver attempts to gain access to the network through a client running the Sygate Protection Agent, depending on the rule set, the protocol driver is allowed, blocked, or a pop-up message displays. See also protocol driver blocking.

Dynamic Host Configuration Protocol (DHCP): A TCP/IP protocol that provides dynamic configuration of host IP addresses and enables individual computers on an IP network to extract configuration parameters from a DHCP server. DHCP lets a system administrator supervise and distribute IP addresses from a central point in the network.

E

EAP: Extensible Authentication Protocol. Sits inside of PPP's authentication protocol and provides a generalized framework for several different authentication methods. EAP is used to pass the authentication information between the supplicant (the wireless workstation) and the authentication server. The actual authentication is defined and handled by the EAP type. The access point acting as authenticator is only a proxy to allow the supplicant and the authentication server to communicate.

encryption: The use of an algorithm to convert typically sensitive data into a form that is unreadable except by authorized users. See also Communications Channel Encryption.

endpoint: Any network device that connects to the enterprise network and runs network-based applications. Network devices can include laptops, desktop computers, and servers. See also access point.

Endpoint Enforcement: The ability of the Sygate Protection Agent to execute Host Integrity rules independent of the Sygate Enforcer. The Agent can take an action if the Host Integrity rules fail, block access to the enterprise network by switching to a quarantine location, and then initiate the appropriate restorative action. Also called “self-enforcement.”

enforcement: To compel observance of security policies or obedience to Host Integrity rules at all enterprise network endpoints and access points. Sygate software automates the enforcement of corporate security policies by linking users, devices, and applications to trusted network communication. Sygate Agent software can be installed on every device to provide policy enforcement capabilities across the enterprise. If the Agent attempting access fails to meet the security requirements, an action occurs that blocks the Agent from accessing the network. See also VPN enforcement, Endpoint Quarantine, wireless enforcement.

Enforcer: See Sygate Enforcer.

environment specifications: Information, such as registry settings, applications that are running, file attributes (such as age, size, version, etc.). Environment specifications are used for the Host Integrity settings.

environment variable: A string that is defined in relation to the current environment, such as a drive, path, or file name, associated with a symbolic name that can be used by Windows. Using an environment variable instead of a fixed value lets you create rules or specify programs allowing for variations of some information. To list environment variables on Windows, type “set” at the command line.

excluded hosts: A list of hosts for which all traffic going to and coming from is ignored by Agents.

F

failover: A standby operation that automatically switches to a standby system if the primary system fails. Failover automatically redirects requests from the failed system to the standby system. For example, you can install multiple Sygate Enforcers and Sygate Policy Managers on different machines to achieve failover. If one of the machines fails, another Policy Manager or Enforcer, which is installed on a separate machine, automatically connects clients to the corporate network. See also database replication.

file fingerprint: A 128-bit number or checksum that represents an executable file. See also file fingerprint lists.

file fingerprint lists: Lists of checksums of executables created using a tool called checksum.exe provided with the Protection Agent software. For use with System Lockdown and OS Protection. See also file fingerprint.

filtering logs: Viewing selected information from logged information. For example, a filter can be set up so that you can view only blocked traffic, critical information, or logged events occurring during the past day. See also logs.

firewall: Hardware, software, or a combination of both that is used to prevent unauthorized Internet users from accessing a private network. All information entering or leaving a network must pass through a firewall, which examines the information packets and blocks those that do not meet security criteria. The Sygate Protection Agent component of Sygate Enterprise Protection Allows, Blocks, or Asks whether incoming traffic is allowed to access an organization's network or resources. By using firewall rules, an Agent can systematically allow, block, and ask questions of incoming traffic from specific IP addresses and ports. See also firewall rule, Sygate Protection Agent.

firewall rule: A stipulation that helps determine whether or not a computer can gain access to a network (Sygate Enterprise Protection only). For example, a firewall rule may state "Port 80 is allowed." A type of rule that enables a system administrator to create security rules without having to define priorities, severities, triggers, and events. Examples of rules could be a rule that allows trusted applications, a rule that allows hosts, a rule that allows VPNs, etc.

fragmented packets: A packet that is broken into smaller parts to send a packet more efficiently through an organization's network or Internet. When Allow Fragmented Packets is enabled on the Policy Manager, the Agent automatically allows the fragmented packets. See also packet.

G

Gateway Enforcer: Used for enforcement at access points for external computers connecting remotely through a VPN, Wireless LAN, or Remote Access Server (RAS). It can block access to clients unless they are running a Sygate Agent and comply with Host Integrity requirements.

Global group: The uppermost group on a network that contains the Computers root group and the Users root group. It contains and controls the properties of all Agents on a network. All other groups automatically inherit the security policy of the Global group. See also Computer group, groups, inheritance, Users group.

groups: All users and computers on an enterprise network are organized into groups with similar security needs and settings. Computer and Users Groups are created and maintained by a system administrator on the Sygate Policy Manager. A group cannot be edited unless it is locked or checked-out first making it so only one administrator can make changes to it at any time. See also Computer group, Users Group, Global Group.

GUID: Global Unique Identifier. See unique ID.

H

heartbeat: The frequency with which Agents or Sygate Enforcers communicate with the Sygate Policy Manager to check for new security policies and upload the latest logs. Heartbeats between the Enforcer and the Policy Manager occur in regular intervals (set by the system administrator). Agents can also check for updated Agent software.

hijack: A type of attack where an intruder takes control of an existing communication session between a server and a legitimate user who has connected and authenticated with the server. The intruder can monitor the session passively recording the transfer of sensitive information such as passwords and code. Another type of hijacking involves an active attack done by forcing the user offline (with a Denial of Service attack) and taking over the session. The intruder begins acting like the user, executing commands, and sending information to the server.

Host Integrity: The ability to define, enforce, and restore the security of clients to secure enterprise networks and data. Host Integrity rules can be set up to verify that Agents attempting network access are running antivirus software, patches, and hot fixes and other application criteria. See also Host Integrity policy, Host Integrity check, Sygate Enforcer.

Host Integrity check: The Host Integrity policy settings that you set up are implemented by the Sygate Agent running a Host Integrity check. During the Host Integrity check, the Agent follows the requirements set in the Host Integrity policy to examine the registry keys, running applications, or date and size of a file. If required software, patches and hot fixes have not been installed on the computer, the Agent can be set to connect to an update server to download and install the required software.

Host Integrity policy: Host integrity policies specify the exact software required to be running on the client computer, for example, security applications such as firewall or antivirus software, antivirus signature file updates, version information, and operating system patches and service packs.

Host Integrity restoration: An option that allows an automatic system update, if needed. Working together with an Enforcer, Host Integrity rules can be set up to verify that Agents attempting access are running antivirus software, patches, hot fixes, and checking specified registry key values, then update an Agent's system and files automatically if they are out-of-date.

I

ICMP: See Internet Control Message Protocol (ICMP).

icon: A small visual image displayed on a computer screen to represent an application, a command, an object, or to indicate status. On the Sygate Policy Manager, icons show when Agents are online and represent groups, users, and computers. Icons shown on screens in Sygate software are also used to display status. For example, in the Sygate Secure Agent interface, blinking blue lights indicate incoming and outgoing traffic.

IDS: See Intrusion Detection System (IDS).

inbound traffic: Traffic that was initiated from a remote computer. See also outbound traffic.

inheritance: A way of implementing security policies, which include rules and settings, across groups and subgroups of users and computers. Security policies can be created globally so that they filter down to all subgroups. Traits that can be inherited include all rules, IPS rules, Host Integrity rules, locations (except default locations, which are not inherited), and group settings. See also rule inheritance.

Internet Control Message Protocol (ICMP): An Internet protocol (defined in RFC 792) that is primarily for reporting errors in TCP/IP messages and exchanging limited status and control information.

Internet Information Services (IIS): Web services software from Microsoft that is the Hypertext Transport Protocol (HTTP) server for the Microsoft Windows platform. Microsoft IIS is required on the Sygate Policy Manager in order for the Policy Manager to be installed successfully.

Intrusion Detection System (IDS): A device or software that detects and notifies a user or enterprise of unauthorized or anomalous access to a network or computer system. Sygate's IDS operates on every machine in an enterprise where the Sygate Protection Agent is installed by analyzing network packets targeted at the network node and comparing them with signature database entries. An IDS helps identify attacks and probes by monitoring traffic for attack signatures that represent hostile activity. Sygate's software includes Intrusion Protection as well as Intrusion Detection. See also Intrusion Prevention System (IPS).

Intrusion Prevention System (IPS): Sygate Enterprise Protection only. A device or software used to prevent intruders from accessing systems from malicious or suspicious activity. This is contrast to an Intrusion Detection System (IDS), which merely detects and notifies. Sygate Protection Agent is both an IDS and an IPS product since the Agent includes both an IDS and firewall functionality making it capable of not only detecting but also blocking an attack. See also Intrusion Detection System (IDS).

IP address: A 32-bit address used to identify a node on a network. Each node on the network must be assigned a unique address in dotted decimal notation, such as 125.132.42.7. See also local IP address, remote IP address.

IP fragmentation: A packet that has been split into two or more packets. The Sygate Protection Agent supports IP fragmentation, the ability to receive or send incomplete packets over the network. See also packets, fragmented packets.

IP spoofing: IP spoofing is a process where an intruder uses an IP address of another computer to acquire information or gain access. Because the intruder appears to be someone else, if a reply is sent, it goes to the spoofed address, not the intruder's address.

IPS: See Intrusion Prevention System (IPS).

L

LAN Enforcer: Used for enforcement for internal clients that connect to the LAN through a switch or wireless access point that supports 802.1x authentication. The LAN Enforcer authenticates clients to ensure they are running the Sygate Agent and comply with Host Integrity requirements. The LAN Enforcer can work with or without a RADIUS server that provides user-level authentication.

LAN Sensor: A Protection Agent set up as a LAN Sensor detects new devices connecting to the network and sends this information to the Policy Manager, which can then generate a report related to new devices. Sygate Enterprise Protection only.

LDAP: See Lightweight Directory Access Protocol (LDAP).

Learned Applications: An application that has been launched by an Agent and is tracked in a master list on the Policy Manager. The master list includes all applications that any Agent has run. A system administrator can look up a specific application and see all the Agents that have used it. See also application authentication, Application Learning.

Learned Applications list: The master list of applications that have been launched by Agents. The list can be viewed from the Policies tab of the Policy Manager by using the Learned Application Query tool. See also Application Learning.

library: See signature library, System Library, custom library.

license: Permission to use specific Sygate components or features. When purchasing Sygate Enterprise Protection or Sygate Network Access Control software, a registration code includes licenses for components such as Sygate Policy Managers, Enforcers, Agents, Event Logger, and other licensed features that were ordered (including features such as Power User Mode, Host Integrity, and Intrusion Detection).

Lightweight Directory Access Protocol (LDAP): A standard directory access protocol for searching and updating information directories containing, for example, email addresses, phone numbers, and computer names and addresses. LDAP is the primary protocol used to access directory servers such as Active Directory. See also Active Directory, directory server.

local database: An embedded or SQL database that is installed on the same computer as the Sygate Policy Manager. If using the embedded database, it is always installed locally. See also remote database.

local IP address: From the perspective of the Agent, the IP address of the computer the user is working on. See also IP address.

local port: From the perspective of the Agent, the port on the computer being used for this connection. See also port.

local site: The Policy Manager whose console you are logged in to.

location: A set of rules and regulations called an adaptive security policy that the Sygate Policy Manager sends to each Sygate Agent whenever the Agent sends a request to the Policy Manager. Location is defined by the network settings of the computer where the request was initiated. See also network settings.

Log Damper: An option that causes the Sygate Protection Agent to log only one event if multiple similar events happen in a relatively short time frame. This protects the Agent from being inundated by hundreds or thousands of simultaneous events as might happen in a DoS attack. For example, if a thousand packets are received in one second, by dampening the log, the Agent logs one entry that shows that the event occurred a thousand times. See also logs.

logs: Files that store information about activities that occurred on the system. Sygate Policy Manager provides extensive logging capabilities for tracking events such as security violations, changes to security policies, network traffic, client connections, and administrative activities.

lsass.exe: A Local Security Authority Service Executable and Server DLL on the Windows operating system. It is a Windows security mechanism used to verify user logins.

M

MAC address: A vendor's Media Access Control hardware address that identifies computers, servers, routers, or other network devices. See also Anti-MAC Spoofing.

MAC Spoofing: Intruders use a technique called MAC (media access control) spoofing to hack into a victim's computer by using the MAC address of another computer to send an ARP (Address Resolution Protocol) response packet to the victim even though the victim did not send an ARP request. The victim host renews the internal ARP table using the malicious ARP response packet. See also Anti-MAC Spoofing.

mapisp32.exe: Microsoft Windows Messaging Subsystem Spooler, allows mail applications to use a standard Messaging Application Program Interface (MAPI) to access messages, addresses, and transport services.

MD5 hash: RSA Data Security, Inc. MD5 Message-Digest Algorithm: A one-way function that produces a unique 128-bit value. MD5 hashing transforms information and produces a value that it cannot be changed back into its original form. This method is used for encrypted authentication (for example, verifying passwords or authenticating applications).

mstask.exe: The Task Scheduler engine used by the Windows operating system.

multicast: Sending a message simultaneously to more than one destination on a network. See also broadcast, unicast.

N

NetBIOS protection: An option on the Policy Manager that blocks all communication from computers located outside a client's local subnet range. NetBIOS traffic is blocked on UDP ports 88, 137, and 138 and TCP ports 135, 139, 445, and 1026. See also subnet.

network adapter: A device that connects a computer to a network.

network interface card (NIC): A device that is installed in a computer that provides the ability to communicate with other connected devices on the network.

network settings: Settings that determine the location (policy) of an Agent attempting to gain access to the network. Network settings can check MAC or IP address, DNS server IP address, WINS Server IP address, IP range, Sygate Policy Manager connection, and type of connection (VPN or dial-up networking). They are used for AutoLocation switching. See also AutoLocation Switching.

ntoskrnl.exe: NT Kernel & System, a standard Windows service that initializes the kernel and drivers needed during a session.

O

OS Fingerprint Masquerading: Sygate Enterprise Protection only. An advanced firewall policy setting that keeps programs from detecting the operating system of a computer running the Agent. When OS Fingerprint Masquerading is enabled, the Protection Agent modifies TCP/IP packets so it is not possible to determine its operating system.

OS Protection: Policies that provide protection such as file protection, registry protection, process execution protection, and application execution control (Sygate Enterprise Protection only). See also OS Protection templates.

OS Protection templates: OS Protection policies developed specifically by Sygate to harden desktop computers or servers such as Apache, DHCP, IIS, or SQL servers. If your license includes Online Subscription, you can access new templates as they made available by Sygate. See also OS Protection.

outbound traffic: Traffic that was initiated from the local computer. See also inbound traffic.

P

packet: A unit of data sent over a network. A packet header that includes information, such as the message length, priority, checksum, as well as the source and destination address, accompanies it. When packets are sent over a network protected by Sygate software, each packet is evaluated for specific patterns that indicate known attacks. See also fragmented packets.

policy: See security policy.

Policy Manager list: A list that includes all Policy Managers that Agents and Enforcers can connect to after installation. The lists are ordered by priority.

port: A connection on a computer where devices that pass data to and from the computer are physically connected. Ports are numbered from 0 to 65535. Ports 0 to 1024 are reserved for use by certain privileged services. See also Authentication port, local port, remote port, source port.

port scan: A method that hackers use to determine which computer's ports are open to communication. It is done by sending messages to computer ports to locate points of vulnerability. Although it can be a precursor to an intrusion attempt, port scanning does not in itself provide access to a remote system. See also Portscan Checking.

Portscan checking: An Intrusion Prevention option on the Sygate Policy Manager that monitors all incoming packets that are blocked by any security rule. If several different packets were blocked on different ports in a short period of time, a security log entry is generated. Portscan Checking does not block any packets. A security policy needs to be created to block traffic in the event that a port scan occurs.

Power User Mode: A Protection Agent feature that allows a privileged user, or a user with elevated rights, to customize security settings on their individual computer while allowing the Policy Manager to maintain partial control over their computer configuration. See also Client Control, Server Control.

preshared secret: An encryption key used to secure the communication channel between the Policy Manager, Agents, and Enforcers. Agents can communicate with Policy Managers having the same preshared secret. All Policy Managers at all sites should use the same preshared secret (in case users travel from site to site). The preshared secret is included in the Agent package, so that the Agent can connect to the Policy Manager.

profile: See security policy.

Profile Serial Number: A number that a Policy Manager automatically generates every time an Agent's security policy changes.

protocol driver blocking: A security measure that blocks malicious applications from using their own protocol driver to exit the network surreptitiously.

R

remote database: An SQL database used for storing Sygate data that is installed on a different computer from the one on which the Sygate Policy Manager is installed. See also local database.

remote IP address: The IP address of a computer to which information is being transmitted.

remote port: A port on another computer attempting to transmit information over a network connection.

replication: See database replication.

replication partner: A site whose database contains the same information as another site. Replication is set up during Policy Manager installation or reconfiguration.

reports: A group of records defined by a set of criteria that is summarized and organized into readable documents. Generated reports can include real-time information, such as all alerts, logins, accepted and blocked clients, executed applications, and other summaries.

restoration: See Host Integrity restoration.

RSA ACE Server: A server used to verify RSA SecurID Login authentication requests and to administer policies for enterprise networks.

RSA SecurID Login: RSA SecurID uses two-factor authentication: a code you know (a PIN), and an item you have (a PIN pad, “smartcard,” or software token), and then generates a one-time login code that is usable for a period of 60 seconds. After that period, the combination of the PIN and the smartcard will generate another, completely different one-time login code.

rule inheritance: The process whereby a rule that is applied to a parent group is automatically applied to any subgroups. Rule inheritance applies to Firewall Rules, Host Integrity Rules, and intrusion prevention. For example, any rule applied to the Global group also holds for all Computers and Users on the enterprise network. The rule can only be altered at the Global group level. Rules applied at the Users level, apply to all of the user clients on the system.

S

security alerts: A notification indicating that the Sygate Protection Agent has detected an attack against the client computer.

security policy: A combination of all the security rules and settings that have been applied to a specific group to protect an enterprise’s computing integrity. Security policies can include rules concerning the permitted applications, connection type, VPN, Ethernet, wireless, and any other restrictions or specifications that an organization wants to enforce.

Security Type: A field that provides information on whether or not a Host Integrity check has passed or failed.

self-enforcement: See Endpoint Quarantine.

server: A computer on a network that manages network resources for one or more clients. In the context of Sygate software, it is considered to be the computer having the Sygate Policy Manager installed on it. Sygate documentation refers to this as the Policy Manager. See also Sygate Policy Manager.

Server Control: Setting up the Sygate Protection Agent or Sygate Enforcer in such a way that the client profiles and settings are configured and controlled on Sygate Policy Manager. This option provides for more centralized administrative control than the Client Control option (on the Agent) or the Console Control option (on the Enforcer). See also Client Control, Console Control.

service: A network port, a UDP port, an IP protocol type, or an ICMP type.

services.exe: Services and Controller application, a standard controller that manages many Windows services.

signature: A rule that defines how to identify an intrusion. Sygate's Intrusion Prevention System identifies known attacks by pattern-matching against rules or 'signatures' stored in the System Library or a custom library. See also signature library, System Library.

Signature File Serial Number: A number that the Sygate Policy Manager assigns to signature files each time they are updated.

signature library: A set of IPS signatures. Sygate provides a library of known signatures in the System Library, which can be kept up-to-date by downloading the latest version from Sygate automatically (if your license include Online Subscription). Administrators can also specify new attack signatures of their own choosing in custom libraries. See also System Library.

Silent mode: The ability to hide the Sygate Agent user interface from the end user so that it runs silently.

site: One or more Sygate Policy Managers, one Policy Manager database, optionally one or more Sygate Enforcers, and the clients that connect to the Policy Manager. The local site is the Policy Manager that you are logged on to and administrators can view remote sites from the local site.

Smart DHCP: A smart traffic filtering option that allows a Dynamic Host Configuration Protocol (DHCP) client to receive an IP address from a DHCP server while protecting the client against DHCP attacks from a network. If a Sygate Protection Agent sends a DHCP request to a DHCP server, it waits for five seconds to allow for an incoming DHCP response. If a Sygate Protection Agent does not send a DHCP request to a DHCP server, then Smart DHCP does not allow the packet. Smart DHCP does not block packets. It simply allows the packet if a DHCP request was made. Any other DHCP blocking or allowing is done by the normal security rule set. See also Dynamic Host Configuration Protocol (DHCP).

Smart DNS: A smart traffic filtering option that allows a Domain Name System (DNS) client to resolve a domain name from a DNS server while providing protection against DNS attacks from the network. This option blocks all Domain Name System (DNS) traffic except outgoing DNS requests and the corresponding reply. If a client computer sends a DNS request and another computer responds within five seconds, the communication is allowed. All other DNS packets are dropped. Smart DNS does not block any packets; blocking is done by the normal security rule set.

Smart Traffic Filter: Associated with a firewall policy, allows specific types of traffic that must be permitted on most networks such as DHCP, DNS, and WINS traffic. See also Smart DHCP, Smart DNS, Smart WINS.

Smart WINS: A smart traffic filtering option that allows Windows Internet Naming Service (WINS) requests only if they have been requested. If the traffic is not requested, the WINS reply is blocked.

sniffing: The process of actively capturing datagram and packet information from a selected network. Sniffing acquires all network traffic regardless of where the packets are addressed.

source IP address: The IP address from which traffic originated. See also IP address.

source port: The port number from which traffic originated. See also port.

spoofing: A technique used by an intruder to gain unauthorized network access to a computer system or network by forging known network credentials. IP spoofing is a common method for intruders to gain unauthorized network access to a computer systems or network.

Stealth Mode Browsing: Sygate Enterprise Protection only. An advanced firewall policy setting that detects all HTTP traffic on port 80 from a web browser and removes information such as the browser name and version, the operating system, and the reference web page. It stops web sites from knowing which operating system and browser you are using. Stealth Mode Browsing may cause some web sites not to function properly because it removes the browser signature, called the HTTP_USER_AGENT, from the HTTP request header and replaces it with a generic signature.

subnet: Portions of a TCP/IP network used to increase the bandwidth on the network by subdividing the network into portions or segments. All IP addresses within a subnet use the same first three sets of numbers (such as 192.168.1 in 192.168.1.180 and 192.168.1.170) indicating they are on the same network. A subnet is See also subnet mask.

subnet mask: A value that allows a network to be subdivided and provides for more complex address assignments. The subnet mask format is nnn.nnn.nnn.nnn, such as 255.255.255.0.

svchost.exe: Generic Host Process for Win32 Services, a generic host process for services that are run from dynamic link libraries (DLLs). It checks the services portion of the registry to create a list of services it needs to load. Multiple instances of Svchost.exe may be running at the same time.

Sygate Enforcement Agent: Software that you deploy on company computers to enforce Host Integrity policies and automate restoration of compliance to policies. See also Host Integrity, Sygate Network Access Control.

Sygate Enforcer: A software component that enforces policy compliance in three ways: Gateway Enforcer, DHCP Enforcer, or LAN Enforcer. Enforcers authenticate clients to ensure they are running the Sygate Agent and comply with Host Integrity rules. A Gateway Enforcer is used for enforcement at access points for external computers connecting remotely through a VPN, Wireless LAN, or Remote Access Server (RAS). A LAN Enforcer is used for enforcement for internal clients that connect to the LAN through a switch that supports 802.1x authentication. A DHCP Enforcer is used for enforcement of internal clients that gain access to the LAN by receiving a dynamic IP address through a Dynamic Host Configuration Protocol (DHCP) server.

Sygate Enterprise Protection: A software suite that includes the Sygate Policy Manager, Sygate Protection Agents, and optionally, Sygate Enforcement Agents, and one or more Sygate Enforcers. It protects wireless, VPN and wireless connected laptops, workstations, and servers with firewall, intrusion detection, and policy enforcement. See also Sygate Protection Agent, Sygate Enforcer, Sygate Policy Manager, Sygate Network Access Control.

Sygate Network Access Control: A management, deployment, and enforcement system for Host Integrity security policies. Host Integrity refers to the ability to define, enforce, and restore the security of clients (hosts) in order to secure enterprise networks and data. See also Sygate Enterprise Protection.

Sygate Personal Firewall: A consumer host-based firewall whereby the users define their own security policies. See also Sygate Protection Agent.

Sygate Policy Management Console: Any computer you want to use to log on to the Policy Manager can be used as a remote console provided that it meets system requirements. The Sygate Policy Management Console enables a system administrator to connect to the Policy Manager from other computers or from the Policy Manager itself.

Sygate Policy Manager: A centralized point of control over all Sygate Agents and Enforcers that enables network administrators to define and distribute security policies, collect logs, and maintain the integrity of the corporate network. Also referred to as the Policy Manager in Sygate documentation. See also Sygate Protection Agent, Sygate Enforcement Agent.

Sygate Protection Agent: Sygate Enterprise Protection only. Software component that enforces rule-based security on devices, whether remote or behind a corporate firewall, using security policies defined on the Sygate Policy Manager. Also referred to as the Agent in Sygate documentation. The Agent must be installed on every device before it can connect to the enterprise network. The Agent can detect, identify, and block known Trojans and Denial of Service attacks, and also protects against new or unknown attacks by blocking applications and traffic that violates a defined set of security policies. Port scans are also detected and logged to alert users and system administrators of potential attacks, while maintaining system security.

synchronization: Refers to automatically keeping directory servers up-to-date with the user database including synchronizing between LDAP, Active Directory, and NT Domain. System administrators can specify how often to synchronize the user database with the directory server. See also Active Directory, Lightweight Directory Access Protocol (LDAP).

System Library: A Sygate library containing preconfigured IPS signatures to help detect and prevent known attacks. System administrators can use the System Library or create custom IPS signatures to be included in custom IPS signature libraries on the Sygate Policy Manager. The System Library is shown using a blue icon in the interface. Sygate periodically provides an updated System Library which is available if your license has Online Subscription. See also custom library, signature library.

System Lockdown: A feature of Sygate Enterprise Protection that lets you restrict the programs including DLLs and executables that users running the Protection Agent can run on their computers. See also OS Protection.

T

Transmission Control Protocol/Internet Protocol (TCP/IP): Internet protocols that every Internet user and every Internet server uses to communicate and transfer data over networks. TCP packages data into packets that are sent over the Internet and are reassembled at their destinations. IP handles the addressing and routing of each data packet so it is sent to the correct destination.

trigger: An event that causes a firewall rule to take effect (Sygate Endpoint Prevention only). When creating rules, you can assign specific triggers, which cause Protection Agents to react in a specific way, and actions, which specify what to do when the trigger takes place. For example, you can block all traffic originating from a certain IP address or block traffic during certain hours of the day. Triggers can be linked to specific applications, hosts, schedules, and services.

Trojan, Trojan horse: An application that carries out an unauthorized function covertly while running an authorized application. It is designed to do something other than what it claims to and frequently is destructive in its actions. If this Intrusion Prevention feature is enabled, Sygate Agents can automatically detect and terminate known Trojan horse applications before the Trojan attempts to communicate.

trusted IP address: An IP address permitted access the enterprise network without running the Sygate Agent. See also IP address.

Trusted Platform Module (TPM): An integrated security module that provides protection of sensitive data, individual platform authentication, hardware-protected key generation, random number generation, hash and digital signature, and a platform trust state.

U

UDP: See User Datagram Protocol (UDP).

unique ID: A 128-bit hexadecimal number, also called the GUID, assigned to uniquely identify a client running Sygate Agent software. The unique ID is generated by the Sygate Policy Manager when the Agent is installed.

Universal Enforcement API: An Application Programming Interface that provides functions that allow security-related vendors other than Sygate to integrate their technology with Sygate software. Sygate's Universal API provides information about the status of system components (Agents, Policy Managers, etc.) to the VPN vendors.

User Datagram Protocol (UDP): A communications protocol for the Internet network layer, transport layer, and session layer that uses the Internet Protocol (IP) when sending a datagram message from one computer to another. UDP does not guarantee reliable communication or provide validated sequencing of the packets.

Users group: A set of user clients with similar security requirements. Clients in Users groups have security policies that relate to an user that is connecting to the enterprise network. See also client, Global group, Computer group.

V

virtual private network (VPN): A secure network connection that connects different corporate network sites, allows remote users to connect to an enterprise network, and allows controlled access to different corporate networks. Although a VPN provides a secure tunnel for network traffic, it leaves connection points open to attack. Working with a corporate VPN server, Sygate Enforcer ensures that only computers running a valid security policy of the Sygate Protection Agent can gain access to an enterprise network through a VPN. See also VPN enforcement.

virus: A program that is designed to spread from computer to computer on its own, potentially damaging the system software by corrupting or erasing data, using available memory, or by annoying the user by altering data. A virus is designed to replicate. Generally, it is spread by infecting other files.

VPN enforcement: A way to verify that VPN users are running the Sygate Agent and meet the security requirements before being granted access to the network. See also enforcement, virtual private network (VPN).

VPN Enforcer: See Sygate Enforcer.

W

web console: See Sygate Policy Management Console.

WINS: Short for Windows Internet Naming Service, a system that determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. Determining the IP address for a computer is a complex process when DHCP servers assign IP addresses dynamically. For example, DHCP can assign a different IP address to a client each time a computer logs into the network. WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

wireless access point (wireless AP): A network connection that allows a computer or user to connect to an enterprise network without the use of a hardwired connection to the network. See also access point, end point.

wireless enforcement: A way to verify that users connecting to the network by means of wireless technology are running the Sygate Agent and meet the security requirements before being granted access to the network. See also enforcement.

Wireless Enforcer: See Sygate Enforcer.

worm: A type of computer virus that can replicate itself over a computer network and perform destructive tasks such as using up computer memory resources. Worms do not infect other files as viruses typically do, but instead worms make copies of themselves over and over depleting system resources (hard drive space) or depleting bandwidth (by spreading over shared network resources). See also virus.

Index

A

advanced application rules	
applications tab	59
general tab	53
hosts tab	55
ports and protocols tab	56
scheduling tab	58
applications	
advanced options	37
setting access	36

B

backtracing logs	73
------------------------	----

C

control mode	
determining	8

I

ICMP scan	35
-----------------	----

L

locations	
changing	29
determining	8
logs	
about	63
backtracing	73
behavior log	71
clearing	72
enabling	72

filtering	75
packet log	66
saving	75
system log	68
traffic log	65
viewing Logs	64

M

menus	
client control	17
power user	17
server control	17
messages	
pop-up	79, 80
security	85
warning	86

O

options	
accessing	40
availability	8
email notification tab	48
general tab	41
IEEE 802.1x authentication tab	52
log tab	50
network neighborhood tab	43
security tab	44

P

pop-up messages	
about	79
profiles	
exporting	30

importing.....	30
protection agent	
installing	2
receiving.....	1, 2
starting.....	11
uninstalling.....	3

Q

quick scan	35
------------------	----

R

rules	
advanced	53
application.....	37
viewer	30

S

scanning your system	
accessing	34
types of	35
security rule viewer.....	30
stealth scan.....	35

T

TCP scan.....	35
trojan scan.....	35

U

UDP scan.....	35
---------------	----